VYSOKÁ ŠKOLA BÁŇSKÁ – TECHNICKÁ UNIVERZITA OSTRAVA
EKONOMICKÁ FAKULTA

KATEDRA APLIKOVANÉ INFORMATIKY

Zabezpečení prvků lokální počítačové sítě v malé firmě

Security of Local Area Network's Elements in a Small Company

Student: Aneta Vedralová
Vedoucí bakalářské práce: Ing. Petr Rozehnal, Ph.D.

Ostrava 2013

VŠB - Technická univerzita Ostrava
Ekonomická fakulta
Katedra aplikované informatiky

Zadání bakalářské práce

Student: **Aneta Vedralová**

Studijní program: B6209 Systémové inženýrství a informatika

Studijní obor: 6209R001 Aplikovaná informatika

Téma: Zabezpečení prvků lokální počítačové sítě v malé firmě
Security of Local Area Network's Elements in a Small Company

Zásady pro vypracování:

1. Úvod
2. Východiska řízení bezpečnosti v lokální počítačové síti
3. Popis stávající počítačové sítě a jejího zabezpečení
4. Analýza a návrh zabezpečení, zhodnocení řešení
5. Závěr

Seznam použité literatury
Seznam zkratek
Prohlášení o využití výsledků bakalářské práce
Seznam příloh
Přílohy

Seznam doporučené odborné literatury:

KÁLLAY, Fedor a Peter PENIAK. *Počítačové sítě a jejich aplikace.* 2. vyd. Praha: Grada, 2003. ISBN 80-247-0545-1.
LUDVIG, Miroslav a Bohumír ŠTĚDROŇ. *Teorie bezpečnosti počítačových sítí.* Kralice na Hané: Computer Media, 2008. ISBN 978-80-86686-35-6.
THOMAS, Thomas M. *Zabezpečení počítačových sítí: bez předchozích znalostí.* Brno: CP Books, 2005. ISBN 80-251-0417-6.

Formální náležitosti a rozsah bakalářské práce stanoví pokyny pro vypracování zveřejněné na webových stránkách fakulty.

Vedoucí bakalářské práce: **Ing. Petr Rozehnal, Ph.D.**

Datum zadání: 23.11.2012
Datum odevzdání: 10.05.2013

VYSOKÁ ŠKOLA BÁŇSKÁ - TECHNICKÁ UNIVERZITA Ekonomická fakulta OSTRAVA 1

Ing. Petr Rozehnal, Ph.D.
vedoucí katedry

prof. Dr. Ing. Dana Dluhošová
děkanka fakulty

Poděkování

Chtěla bych poděkovat za vstřícný přístup a odbornou pomoc panu Ing. Petru Rozehnalovi, Ph.D. a panu Ing. Jiřímu Ovčáčkovi při psaní této bakalářské práce. Také bych chtěla poděkovat za odborné rady Marku Štropovi. Dále bych chtěla poděkovat své rodině, která v dobách osobní krize pozvedla mého ducha a dodala mi sílu dokončit tuto práci. Poděkovat bych chtěla i svému příteli Lukáši Jakubovi, který byl jak morální podporou po celou dobu psaní této práce, ale také můj tichý konzultant, jenž nemusel vydat ani hlásku a prozradil mi veškerá řešení. A nakonec patří velké dík i Emmě, která na mě při psaní dávala pozor.

Obsah

1 Úvod

V dnešní době každá firma používá počítače a jiná zařízení, jako například nejrůznější druhy serverů, zapojených do různě velkých počítačových sítí. Tyto počítače a další komponenty počítačové sítě pak obsahují různá data, která jsou danou firmou získaná nebo vypracovaná. Taková data jsou velice ceněná a drahá, proto je také nutné je chránit tím, že firma bude předcházet různým pohromám či hrozbám a minimalizovat rizika spojená s ohrožením počítačové sítě, počítačových stanic a samotných dat.

Pro předcházení nejrůznějších pohrom, hrozeb a rizik, které firmě hrozí, je nutné nejprve si tyto pohromy, hrozby a rizika uvědomit a specifikovat je. To zahrnuje detailní analýzu hrozeb a rizik, jak samotné počítačové sítě, tak blízkého a širšího okolí této sítě. Následně definovat způsoby, jak se před nimi chránit. Což může zahrnovat samotnou strukturu sestavění počítačové sítě, nejrůznější hardwarové prvky, jako jsou směrovače, firewally, switche a další. Nesmí se zapomenout, že i softwarové bezpečnostní vybavení je nezbytné. Jedná se hlavně o antivirovou ochranu, o samotný operační systém stanic a další softwarové prvky, které zvyšují bezpečnost sítě, jako například virtuální stroje spouštěné pomocí virtualizačního softwaru. V neposlední řadě je také nutné stanovit pravidla a postupy, podle kterých se bude chod firmy řídit. Nakonec je nezbytné nejlepší definované způsoby ochrany praktikovat na danou počítačovou síť a provést zhodnocení této prevence.

Cílem této bakalářské práce je analyzovat prvky počítačové sítě a stávající zabezpečení vybrané firmy, dále podrobně analyzovat rizika, hrozby i zranitelná místa této firmy a z těchto analýz pak vytvořit návrh efektivnějšího zabezpečení prvků dané lokální počítačové sítě.

2 Východiska řízení bezpečnosti v lokální počítačové síti

2.1 Definice, dělení a topologie počítačových sítí a serverů

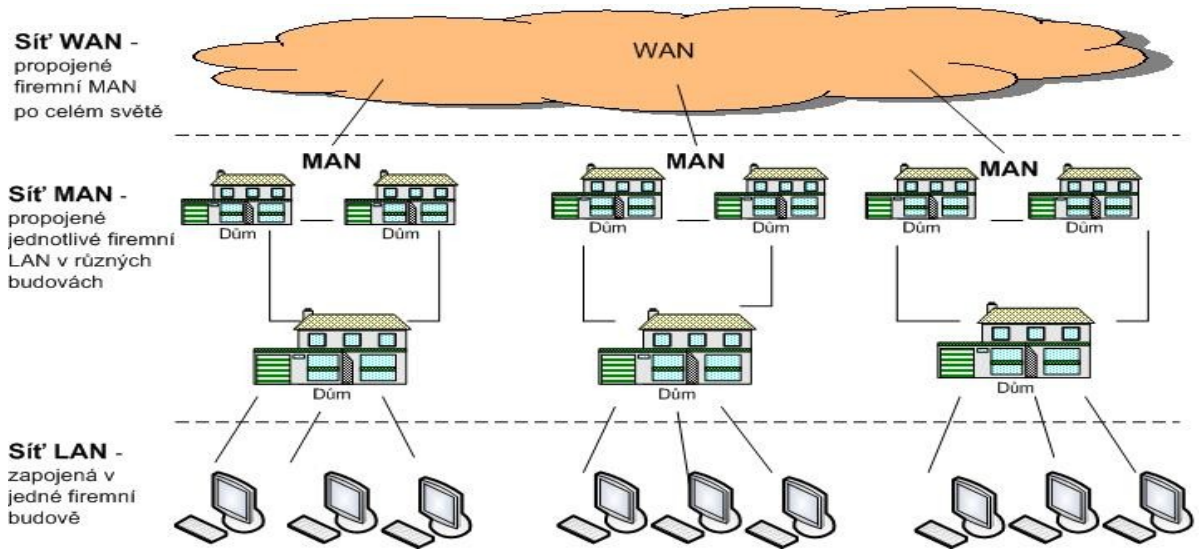
2.1.1 Počítačová síť

„Počítačová síť (PS) představuje obecně systém vzájemně propojených počítačů, terminálů a dalších zařízení, komunikujících prostřednictvím komunikačních subsystémů sítě, přenosných médií a aktivních komunikačních prvků.“ (Kállay a Peniak, s.19, 2011)

Rozdělené sítě podle její rozlehlosti

Rozdělení sítě podle její rozlehlosti a komunikaci mezi jednotlivými typy se zobrazuje na obrázku 2.1.

- **PAN** (Personal Area Network) je to takzvaná dočasná osobní síť. Je rozšířena hlavně v domácnostech. Propojuje hlavně přenosná zařízení, jako jsou notebooky, mobily nebo tablety Používá technologie, jako jsou Wifi, Bluethoot, USB kabel …
- **LAN** (Local Area Network) je považována za menší počítačovou síť. Její dosah pokrývá rozlohu do 10 km (což může být území podniku popřípadě školy). Její součástí je několik desítek počítačových jednotek a jiných uzlů.
- **MAN** (Metropolitan Area Network) pokrývá rozlohu desítek kilometrů, jako je například území města. Je sestavena ze vzdálených lokálních sítí.
- **WAN** (Wide Area Network) je datová sít s neomezeným dosahem. Pokrývá území jednotlivých států či dokonce kontinentů. Skládá se z jednotlivých MAN a LAN. Příkladem WAN je třeba Internet.



2.1 **Rozdělené sítě podle její rozlehlosti (vlastní)**

Rozdělení sítě podle přenosu

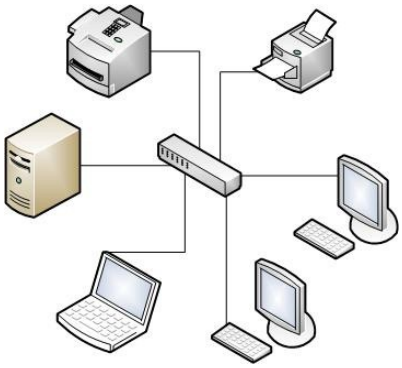
Pelikán (2004) a Sosinsky (2010) tvrdí, že se počítačové sítě dělí z hlediska přenosových médií, na:

- Elektrické vodiče
  - Koaxiální kabel
    - skládá se z měděného jádra (drátu) obaleného izolací, měděnou síťkou a hliníkovým pláštěm
    - používá se pro širokopásmové a vysokorychlostní spoje
    - Výhody a nevýhody Viz Příloha – Tabulky: Tabulka 1
  - Kroucená dvojlinka
    - párové, stíněné, měděné kabely zakroucené do sebe
    - používá se hlavně u starších lokálních sítí.
    - Typy:
      → STP (Shielded Twisted-Pair) – stíněná kroucená dvojlinka
      → UTP (Unshielded Twisted-Pair) – nestíněná kroucená dvojlinka
    - Výhody a nevýhody Viz Příloha – Tabulky: Tabulka 2
- Optický kabel
  - používá se pro moderní vysokorychlostní sítě s velkou kapacitou
  - je produkován v párech – pro každý komunikační směr jedno
  - zakládá se na myšlence úplného odrazu světla
  - Rozdělení:
    - **Jednovidové** (Single-mode) – má tenké jádro, světlo k jádru proudí jen jednou cestou a útlum tohoto světla je mizivý.
    - **Multividové** (Multi-mode) – má masivnější jádro, světlo proudí k jádru více cestami a v přenosu může docházet k šumům na straně příjemce.
- Bezdrátový přenos
  - tento přenos používá vzduch nebo vakuem za pomoci vysílače a přijímače
  - používá vlny na rádiových a mikrovlnných frekvencích
  - využívá tři metody kódování informací

2.1.2 Topologie lokálních sítí

Sosinsky (2010) tvrdí, že topologie LAN zobrazuje způsob zapojení uzlů do sítě. Rozděluje se na logickou topologii a pak tu fyzickou:

- **Sběrnice** (Bus) je založena na zapojení uzlů sítě do jedné řady pomocí koaxiálních kabelů.
- **Kruh** (Ring) je propojení sousedních uzlů sítě tak, aby vytvářely kruh.
- **Hvězda** (Star) v dnešní době je nejpoužívanější, hlavně pro Ethernet. Hlavní roli zde hraje centrální prvek v podobě hubu, switche nebo popřípadě i routeru. Do tohoto centrálního prvku jsou pak zapojeny uzly lokální sítě, jak je to znázorněno v obrázku 2.2.



2.2 Topologie hvězda (vlastní)

- **Rozšířená hvězda** je propojení několika hvězd přes centrální prvky. Toto propojení je hlavně oblíbené ve středních a větších firmách.

2.1.3 Architektury typu peer-to-peer a typu klient/server

Peer-to-Peer je architektura počítačové sítě, ve které není žádná nadřazenost. Uživatelé připojení v této architektuře spolu přímo komunikují. V této architektuře také není žádný centrální uzel počítačové sítě, z kterého by se síť spravovala.

Klient/Server je to tzv. dvouvrstvá architektura. Sosinsky (2010) tvrdí, že v této architektuře serverový systém zpracovává data a dává je k dispozici klientskému systému. Serverový systém komunikuje s klientským pomocí daných protokolů.

2.1.4 Server

Pod serverem si může člověk představit jak počítač, tak i program, který poskytuje určité služby uživatelům. Každý server má své speciální programové vybavení, které určuje jeho bližší funkci. Tato programové vybavení se jinak značí jako síťový operační systém NOS (Network Operating System). *„NOS zabezpečuje vlastní implementaci služeb serverů, komunikaci pracovních stanic se servery a kontrolu a řízení přístupu klientů k příslušným službám serverů (Kállay a Peniak, s. 44, 2011).“*

Rozlišují se dvě implementace NOS:

1) Peer-to-peer (rovný s rovným)
2) Dedicated (dedikovaném)

Při režimu dedicated se umožňuje vykonávání procesu serveru jen na zvláště vymezených uzlech, zatím co v režimu peer-to-peer je podporováno vykovávání tohoto procesu serveru a klientu na jakémkoli uzlu v daného informačního systému. Volba správného režimu záleží na stanovení NOS a dané realizaci LAN nebo WAN. Konečným hlediskem při výběru režimu je vzájemná návaznost funkce serveru a informačního systému. Podle tohoto hlediska rozdělujeme servery na níže uvedené servery.

Souborový server (File Server)

Souborový server zajišťuje dostupnost dat pomocí soustavy souborů a adresářů. *„Jeho funkcí je zabezpečit zápis a čtení souborů na disku serveru podle přidělených přístupových práv jednotlivých uživatelů (Kállay a Peniak, s. 45, 2011).“* Tato přístupová práva jsou formulována v seznamu ACL (Access Control List), což česky znamená seznam pro řízení přístupu. Podle Kallay a Peniaka (2011) se nejčastěji definují práva pro čtení a přepis souboru, změnu parametrů nebo pro vytvoření a smazání podadresáře.

Databázový server

Byly vyvinuty systémy řízení báze dat (SŘBD), protože bylo zapotřebí systému, které dokážou pracovat s velkým množstvím strukturovaných dat (informací). Zejména bylo potřeba rychle k těmto datům přistupovat, prohledávat je a také je třídit.

„Databázové servery jsou specializované uzly sítě zaměřené na databázové operace a funkce systémů řízení báze dat (Kállay a Peniak, s. 46, 2011).“ Hlavním úkolem databázových serverů je provádět zadávání a změnu dat, vyhledávání informací v databázi podle určených znaků nebo kategorizování a indexování informací.

Poštovní server

„Poštovní servery, MTS (Message Transfer System) jsou základním prvkem systému přenosu zpráv a elektronické pošty (Kállay a Peniak, s. 47, 2011).“ Také zabezpečují přenos takzvaných e-mailů i s přílohami v jakémkoli formátu mezi uživateli v síti. Jiří Peterka (© 2011) tvrdí, že se poštovní server skládá z přenosových složek MTA (Massage Transfer Agent), které se starají o samotný přenos zpráv.

Uživatelé pak mají přístup k jednotlivým správám přes klienta elektronické pošty UA (User Agent). Na tomto UA je uživatelům povolena manipulace s danou poštou, jako je např.: vytvoření nové zprávy, odeslání odpovědi na příchozí zprávu, upravení a vymazání jakýchkoli zpráv ve schránce a také uložení zprávy na lokální disk.

Webový server

„WWW (World Wide Web) server je specializovaný prezentační server, zabezpečující přístup klientů k informacím, které jsou uloženy ne formě hypertextových stránek na discích serverů (Kállay a Peniak, s. 49, 2011).“ Tento server využívá protokolu HTTP (Hypertext Transport Protocol), který slouží k vzájemnému přesunu informací. Na webovém serveru jsou dva typy stánek a to statické, které jsou stálé, a dynamické, jsou vytvářeny pomocí aplikačních programů.

Aplikační server

Podle Kallay a Peniaka (2011) se jedná o nový druh serveru, který má za úkol podporovat aplikační služby. Tyto servery se dále zaměřují na distribuované zpracování těchto aplikačních služeb. Aplikační servery poskytují jednotlivým aplikacím své paměťové prostory a čas na zpracovávání a pomáhají se samotným zpracováváním úloh, které jsou řízeny logikou dané aplikace. Současně jsou spojeny s databázovými servery.

2.2 Virtualizační technologie

Horák (2007) ve své knize uvádí, že virtuální technologie jsou v dnešní době velice populární. Jde o technologii, jež umožňuje na jednom fyzickém stroji s operačním systémem aplikovat více tzv. virtuálních strojů. Dokonce v těchto virtuálních stojích umístěných na jednom hardwarovém zařízení mohou být odlišné operační systémy. Jednotlivé vizualizace jsou uskutečňovány pomocí speciálního softwaru (např. VMware, Hyper-V, atd.)

Virtuální technologie se nejčastěji používají pro:

- testování a ladění programů bez toho, aby se instalovala zkušební verze operačního systému,
- prezentaci a výuku, kdy na jednom hardwarovém stroji je možné předvést několik různých operačních systémů současně,
- napodobování provozních podmínek a situací,
- spojení několika serverů bez nakoupení dalšího hardwaru (na jediném fyzickém serveru pracuje více virtuálních serverů).

2.3 Systém řízení bezpečnosti informací (ISMS)

Podle ISO 27000(2010) firmy jakéhokoli typu či velikosti shromažďují, uschovávají a manipulují s velkým množstvím informací, které dále zpracovávají. Dále si tyto firmy

uvědomují, že k dosažení svých cílů je zapotřebí aktiv v podobě informací, souvisejících procesů, počítačové sítě, personálních složek. Každá firma také čelí mnoha rizikům, která ohrožují nebo jinak ovlivňují tato aktiva, a tudíž provádí bezpečnostní opatření, jež má daná aktiva chránit.

„ISMS (Systém řízení bezpečnosti informací) poskytuje model pro ustavení, implementování, zpracování, monitorování, přezkoumávání, udržování a zlepšování ochrany informačních aktiv, aby byly dosaženy cíle organizace na základě posouzení rizik organizace navržených k efektivnímu ošetření a řízení rizik. (ISO 27000, s. 14, 2010)“ Z této definice vyplývá, že ISMS se snaží o ‚dokonalou' bezpečnost, kterou se snaží přizpůsobit pro každou organizaci zvlášť.

2.3.1 Bezpečnost informací

Podle Petříkové (2011) cena dat i jejich správy ve firmách se stále zvyšuje. Bezpečnost informací obsahuje tři primární stránky informačních aktiv, které jsou: důvěrnost, dostupnost a integrita. Podle ISO 27000 (2010) tato bezpečnost informací se uplatní za pomoci kontrol, které se zvolili procesem řízení rizik, a pomocí ISMS, což zahrnuje implementaci určité politiky aktiv, procesů, postupů, organizačních skupin, softwaru a hardwaru.

2.3.2 Postup při zavádění ISMS

Podle Petříkové (2011) a ISO 27000(2010) je postup při zavádění systému řízení bezpečnosti informací následující:

Klasifikace informačních aktiv

Jde o identifikaci hardwaru a softwaru, jiného majetku firem a také na ně kladené bezpečnostní požadavky. S těmito požadavky je spjato posuzování rizik vyplývajících z informačních aktiv, což končí detailní analýzou hrozeb, zranitelností a pravděpodobnost uskutečnění definovaných hrozeb pro informační aktiva. Také se specifikují dopady plynoucí z identifikovaných hrozeb a zranitelností.

Hrozbou se myslí činnosti nebo událost, která je schopna přímo poškodit aktiva uvedené v předchozí kapitole. Tyto hrozby mohou být zapříčiněny jak přírodním faktorem, tak i lidským faktorem a to buďto náhodně nebo úmyslně.

Na druhou stranu zranitelnosti nemusí působit škodu jako takové. První je zapotřebí hrozby, která nalezenou zranitelnost využije.

Posouzení rizik

Pro posuzování rizik, hrozeb, zranitelností a pravděpodobnosti uskutečnění definovaných hrozeb je zapotřebí metody, která může mít specifikované odhady nákladů a výnosů, sociální, ekonomické a přírodní hlediska, zájmy firem, proměnlivé faktory a další vstupní specifikace. Výsledkem uskutečnění této metody by měly být návrhy opatření, které definovaným rizikům předcházejí. Řízení rizik bezpečnosti informací je shrnuto v ISO/IEC 27005 z roku 2009.

Návrh a implementace kontrol bezpečnosti informací

Jedná se o kontroly, které jsou aplikovány pro zajištění redukování identifikovaných rizik na takovou míru, kterou je firma schopna snést. Tyto kontrolní opatření jsou blíže specifikovány v ISO/IEC 27002. Tyto bezpečnostní kontroly závisejí na bezpečnostních požadavcích, které se snaží akceptovat rizika bezpečnostních informací, dále bere v potaz možnosti ošetření daných rizik a nakonec všeobecně přistupují k řízení rizik vybrané firmou.

Sledování, udržování a vylepšování efektivnosti ISMS

Pro samotné zlepšení ISMS a také udržení jeho efektivnosti je nutné tento detailně sledovat a srovnávat výkony s politikou a cíli firmy a pak předložit výsledky tohoto srovnání samotnému managementu firmy. Zkoumání ISMS umožňuje sledovat opravné, preventivní či vylepšující činnosti, zakládající se na výsledcích celkového sledování včetně sledování kontrol bezpečnosti informací.

2.3.3 Přínosy plynoucí z implementace ISMS

Primárním přínosem, který plyne ze zavedení systému řízení bezpečnosti informaci, je podle ISO 27000 (2010) snížení rizik bezpečnosti informací. Z čehož vyplívá, že se jedná i o snížení počtu slabých míst, které se v organizaci vyskytují, nebo také snížení možného dopadu (škody) při nečekaném poškození, zcizení nebo ztrátě dat.

Přínosy podle Petříkové (2010) jsou:

- „S*plnění požadavků národní legislativy,*
- *zajištění přehledu o významných informačních aktivech,*
- *optimalizace nákladů na bezpečnostní opatření,*
- *minimalizace rizika ekonomických ztrát,*
- *zvýšení důvěryhodnosti firmy,*
- *vytvoření základu pro další zlepšování kvality služeb.(Petříková, s.13, 2010)“*

2.4 Firewall, brány, proxy servery a routery

2.4.1 Firewall

Sosinsky (2010) a Thomas (2005) tvrdí, že firewall je vlastně taková obranná zeď, která chrání a izoluje počítačovou síť za ni schovanou před vnějším světem. Tato zeď se pak skládá ze skupiny bezpečnostních opatření. Hlavním prvkem této ochrany je hardwarové zařízení, které oddělí počítavou síť od vnějšího světa. Firewall také umožňuje komunikovat do externí a interní sítě dvěma různými protokoly.

Firewallové skupiny

Sosinsky (2010) a Thomas (2005) tvrdí, že existuje velké množství různých firewallů. Může se jednat o softwarový firewall běžící na hardwarovém zařízení. Může to být software pracující v operačním systému, jako je tomu například u Linuxu, Unixu nebo Windows nebo je to přímo hardwarové zařízení. K vybrání toho správného se musí nejdřív definovat povinnosti hledaného firewallu. Podle nich si pak organizace může vybrat firewall ze skupin firewallů. Sosinsky (2010) uvádí tyto skupiny:

Hardwarové firewally

Jedná se jednoúčelové hardwarové bezpečnostní zařízení s funkcí firewallu. Tato zařízení se dělí na firewally nižší a vyšší kategorie.

Firewally nižší kategorie jsou jednoduché prvky, které fungují hned po zapojení do sítě. Jsou to také zařízení, ve kterých je software stejný jako u modelů vyšší kategorie, ale pro odblokování vyšších funkcí se musí platit licence. Thomas (2005) uvádí jako příklad Cisco 501 a 506.

Firewally vyšší kategorie jsou určeny hlavně pro větší společnosti. Sosinsky (2010) tvrdí, že jsou také zcela odlišné od firewallu nižší kategorie. Jejich hlavními přednostmi je neproniknutelnost, vysoký výkon a vysoká míra dostupnosti. Většina těchto zařízení má v sobě zakomponovanou odolnost proti výpadkům. Což znamená, že má v sobě záložní systém, který při výpadku převezme provoz.

Serverové firewally

Podle Sosinkyho (2010) se jedná o softwarový firewall, který je implementován výrobcem do serverových operačních systémů a pracující nad tímto serverovým operačním systémem. Výhodou je, že není zapotřebí tolik školení a podpory, protože koncový uživatel

zná tento operační systém, hardware lze snadno přizpůsobit požadavkům a je mnoho různých řešení těchto požadavků.

Z pohledu funkčnosti je mezi hardwarovým a serverovým firewallem jen malé množství rozdílů. Serverové firewally jsou lépe implementovány do sítě, mají lepší škálování a jsou lépe dostupné než jiné definované prvky. Hardwarové firewally jsou na druhou stanu lépe vyladěné, proto serverové firewally potřebují řadu hardwaru, aby se vyrovnaly jejich výkonu.

Personální firewally

Těmto firewallům se také říká osobní firewally. Jedná se o firewall chránící jen jeden počítač. Využívá se hlavně v domácnostech. Sosinsky (2010) tvrdí, že i když existuje spousta personálních firewallů. Microsoft má však zabudované vlastní osobní firewally, které byly součástí už v operačních systémech Windows XP.

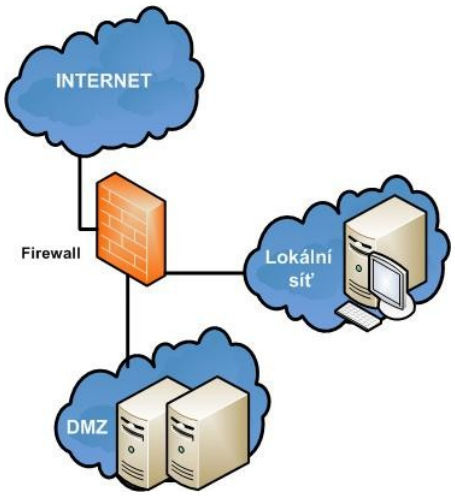
Firewally v routrech

V routrech se často objevují implementované firewally. Toto provedení je příkladem nízkonákladového bezpečnostního zařízení. Podle Thomase (2005) tyto zařízení mají funkci nejen firewallu ale také routeru, ethernetového přepínače a bezdrátového přístupového bodu. Nejčastěji se jedná o součást domácí sítě, kterou nám nainstaloval poskytovatel Internetu, jako součást kabelové nebo DSL linky.

Proxy firewally

„Proxy firewall slouží jako prostředník mezi klientem vně firewallu a systémem nebo serverem uvnitř. (Sosinky, s. 691, 2010)“ Při takovéto komunikaci proxy firewall komunikuje s klientem a systémem nebo serverem zvlášť, jako by to byla dvě spojení. Uživatel tudíž vidí proxy firewall jako koncový bod. Pro zlepšení komunikace může tento typ firewallu použít svou mezipaměť (cache), kterou používá pro často nebo nedávno používaná data nebo ke kontrole platnosti protokolů.

Demilitarizovaná zóna (DMZ)



2.3 Demilitarizovaná zóna (vlastní)

Podle Thomase (2005) se jedná o část sítě, která je umístěna mezi vnitřní sítí (bezpečnou částí sítě) a Internetem (nebezpečnou částí sítě). Tímto způsobem je možné fyzicky izolovat tyto dvě části od sebe a propojit je pouze pomocí skupiny pravidel specifikovaných ve firewallu. Z čehož vyplývá, že z Internetu je možné dostat se jen do demilitarizované zóny a ne do vnitřní sítě. Do této zóny se většinou připojují webové, poštovní a FTP servery, protože tyto servery spolupracují s Internetem.

Demilitarizované zóny docílíme vytvoření třetího rozhraní ve firewallu. Viz obrázek 2.3.

2.4.2 Bezpečnostní brána

Sosinsky (2010) tvrdí, že brána představuje zařízení s funkcí rozhraní mezi dvěma nebo více sítěmi. Mohou se objevovat jak ve formě hardwaru tak jako software, který je instalovaný na servery. Samotná brána pak pracuje na aplikační vrstvě modelu OSI (viz příloha – obrázky: Obrázek 2), ale je schopna fungovat na libovolné vrstvě tohoto modelu jako jsou například prezentační, transportní nebo síťová vrstva, kde může vykonávat další funkce.

2.4.3 Proxy server

Barrie Sosinsky (2010) tvrdí, že se jedná o počítač nebo aplikaci, která vystupuje jako prostředník mezi uživatelem a síťovou službou. Provádí tedy přesměrování, nezpracovává samotné požadavky. Podobně jako u proxy firewallu uživatel vidí jenom proxy server a server taktéž. Tudíž by se dal tento server nazvat branou. Málokdy proxy server dělá jen prostředníka, většinou se zpracování požadavků spojuje s dalšími akcemi. Proxy server je vlastně ‚kříženec' firewallu a brány. Dokáže se tedy spojit s protokolem HTTP, SMTP a FTP, dále také s webovým serverem, poštovním serverem, FTP serverem a také s prohlížečem uživatele.

2.4.4 Směrovač (router)

Microsoft (2013) píše, že směrovač zprostředkovává výměnu informací a komunikaci mezi dvěma a více různými sítěmi. Tyto směrovače se mohou vyskytovat jako kabelové

(s použitím Ethernetového kabelu) nebo bezdrátové. Směrovač se hlavně používá při potřebě Internetu v každém počítači v síti. Směrovač má většinou také vestavěnou bezpečnostní funkci ve formě firewallu a opravdu výkonné směrovače jsou pak ve skutečnosti velmi silné počítače, které provádí velký rozsah zpracovávání dat, což tvrdí Sosinsky (2010).

Thomas (2005) ve své knize zmiňuje, že pokud se řádně směrovač zabezpečí, zvýší se tím i celková bezpečnost celé sítě.

2.5 Uživatelské účty

Díky dnešním vyspělým operačním systémům je uživatelům umožněno střídat se na jedné pracovní stanici. A nemusí to být jen na jedné stanici, ale pomocí uživatelských účtů se dotyčná osoba prokazuje, jestli má nebo nemá povolen přístup do počítačové sítě, potažmo jestli je tato daná osoba zpravomocněna využívat počítačové zařízení umístěné v počítačové síti. Používání uživatelských účtů a hesel je nejrozšířenější bezpečnostní metoda.

2.5.1 Bezpečnost hesla

Bezpečnost hesla je dána jeho složitostí. Tato složitost se řídí podle obecných pravidel, které ve své knize uvádí, jak Thomas (2005), tak i Horák (2003). Tyto pravidla jsou:

- heslo by mělo mít více než osm znaků,
- heslo by nemělo být snadno k nalezení ve slovníku českém nebo i cizojazyčném, n
- hesla by neměla obsahovat:
    - jména známých, mazlíčků, sportovců, sportovních klubů, filmů nebo filmových hvězd,
    - počítačové výrazy nebo jména počítačových firem,
    - snadno odvoditelné řetězce písmen nebo čísel (např.: 123456789, aabbcc, atd.),
    - výrazy, které jsou zmíněny výše, napsané pozpátku,
    - výrazy, které jsou zmíněny výše, a k nim přidat jediné číslo (např.: tatínek1, 5Titanic, …).
- heslo by mělo obsahovat jak malá, tak i velká písmena,
- heslo by mělo obsahovat jiné znaky, jako jsou například: . ! ? ( ) ; : atd.

Pokud je vytvořeno heslo podle těchto pravidel, lze ho označit za ‚silné‘. Takové heslo vypadá podobně jako tento řetězec: 95!ah0J:48R. Takové heslo by ale mělo být také snadno

zapamatovatelné, protože by se hesla neměla nikam psát na papír nebo dokonce ukládat v elektronické podobě.

Podle Thomase (2005) by se měla práce s hesly řídit podle určitých bezpečnostních zásad, které zvýší šanci na ochránění počítačové sítě před zneužitím. Mezi takové zásady patří:

- pravidlo obměny systémových hesel alespoň jednou za čtvrt roku,
- pravidlo obměny uživatelských hesel alespoň jednou za šest měsíců, ale co čtyři měsíce by bylo ještě lepší,
- pravidlo nezapisování hesel do elektronické pošty nebo podobné komunikace,
- pravidlo utajenosti hesla (Pokud někdo bude chtít heslo vědět, uživatel ho nesmí prozradit nebo si vyžádat povolení od bezpečnostního týmu.)
- pravidlo spravování provozních systémových hesel v globální databázi pod správou bezpečnostního týmu,
- pravidlo ‚silných' hesel.

2.5.2 Bezpečnostní skupina

Podle Ministra (2010) bezpečnostní skupiny zásadně pomáhají při stanovování přístupových oprávnění. Jedná se o to, že jednotlivý uživatelé (uživatelské účty) jsou přiřazeny do jednotlivých skupin, u kterých jsou nastaveny tyto přístupové oprávnění. Tudíž se nemusí tyto práva nastavovat u jednotlivých účtů.

Následný postup ukazuje, jak se pracuje s těmito bezpečnostními skupinami:

1) První je důležité vytvořit danou bezpečnostní skupiny.
2) Potom se daným bezpečnostním skupinám přidělí příslušná oprávnění, díky kterým jsou uživatele schopni pracovat s určitými daty nebo využívat určitá zařízení zapojená do dané počítačové sítě.
3) Teprve po vytvoření bezpečnostních skupin a nastavení jejich oprávnění se přiřazují jednotlivý uživatelé (uživatelské účty) do těchto daných bezpečnostních skupin. Tyto uživatelské účty se pak řídí nastavenými právy dané skupiny.

Podle Ministra (2010) platí, že pokud je potřeba nějakému uživateli odebrat přístup (práva) k jistým datům nebo zařízením, nemůžou se jen u tohoto uživatele odstranit příslušná práva, ale musí se vyřadit ze skupin, které mají k těmto jistým datům přístup.

2.6 Šifrování

Sosinsky (2010) označuje šifrování za proces, který danou informaci převede na data, která se nám zdají nesrozumitelná. Dešifrování je tudíž opačný proces, kdy se zašifrovaná data převádí na informace, které jsou člověku srozumitelná.

Někdy je šifrování založeno na takzvaném klíči. Jedná se o informaci, která reprezentuje určitou proměnnou jistého druhu. Ministr (2010) tvrdí, že obtížnost rozluštění informace závisí na délce tohoto klíče (čím delší tím lepší). Klíč jako takový se z pravidla nezveřejňuje, znají ho jen pověřené osoby.

Někdy se vyskytne situace, kdy je zapotřebí více klíčů, jako například u elektronických podpisů. V této situaci se klíče dělí na soukromý a veřejný klíč. Veřejný klíč se sdílí mezi uživateli s oprávněním (odesílatel a příjemce), soukromý klíč však ponechávají v tajnosti. Nejbezpečnější šifra je založena na principu proměnlivého aktuálního klíče.

V dnešní době jsou šifry velice vyspělé a nejdou snadno prolomit. Mezi tři základní šifrovací algoritmy se řadí:

- **DES** (Data Encryption Standart) je to šifrovací algoritmus, který používá symetrické klíče o 56 bitech. Byl to předchůdce 3DES (Triple Data Ecvryption Standart). Dnes je nejnovější algoritmus AES (Advanced Ecryption Standart).
- **Diffie-Hellmanův algoritmus** jedná se o algoritmus, který slouží k šifrování zpráv mezi dvěma uživateli.
- **Algoritmus RSA** (autoři R. **R**ivest, A. **S**hamir, L. **A**dleman) se podle Sosinsky (2010) skládá z generování klíče a samotného šifrování i dešifrování prostřednictvím soukromých a veřejných klíčů. Veřejný klíč slouží k samotnému šifrování informace a jediný způsob jak je znovu rozšifrovat je použití soukromého klíče, který je párový pro daný veřejný kláč.

2.6.1 Symetrické šifrování

Podle Sosinsky (2010) se nejčastěji tyto algoritmy soužívají spolu s blokovými šiframi, proudovými šiframi a hashovacími funkcemi.

Blokové šifry

Tato šifra pracuje s blokem textu. Pomocí klíče se šifra zašifruje a stejně velký text. *„Pokud je délka zprávy větší než délka bloku šifry, algoritmus bere blok za blokem a za pomocí aktuálního bloku a klíče zašifruje následující úsek dat o velikosti jednoho bloku a tak*

dále (Sosinsky, s. 681, 2010).“ Algoritmus tento postup opakuji do té doby, dokud se nezašifruje celá zpráva.

Příkladem blokové šifry jsou algoritmy DES a AES, až na to, že DES se nevyužívá pro vysoce zabezpečenou komunikaci. Je však vyhledávaný pro svou rychlost dešifrování a samotného šifrování. DES se používá například v e-mailových zprávách či bankomatech.

Proudové šifry

Tato šifra pracuje na principu velmi dlouhého klíče, který vytváří symbol po symbolu. Samotný vznik klíče je velice nepředvídatelný proces. Zde také platí pravidlo, které potvrzují autoři Ministr (2010) a Sosinsky (2010), čím delší je klíč, tím je šifra, zde proudová, bezpečnější.

U klíčů proudové šifry jsou základní požadované vlastnosti nahodilost a neopakovatelnost. Jakmile je klíč jednou použitý stává se znehodnoceným. Proto podle Sosinky (2010) proudové šifry nekladou velké požadavky na vytváření klíčů v reálném čase. Příkladem této proudové šifry jsou jednorázové tabulky.

RC4 je nejrozšířenější standart proudové šifry. Je základem pro bezdrátové bezpečnostní protokoly WEP a WPA. Jeho další verze jsou například RC2, RC5 a RC6. Pracuje s proudovými klíči o velikosti mezi 40 až 256 bity. *„Proudový klíč se pak využívá k zašifrování vstupního textu, přičemž hodnoty indexu, které modifikují proudový klíš, jsou inkrementovány s pomocí algoritmu pro generování pseudonáhodných čísel. (Sosinsky, s. 681, 2010)“* Závěrem se aplikuje operace XOR.

Algoritmus RD4 však není bez chyby. Jeho varianta používaná pro bezdrátový protokol WEP s příslušným nástrojem lze prolomit bezmála za minutu.

Hashovací funkce

Je to další algoritmus, který pracuje s klíči. Tento klíč pak nazýváme hashovací funkcí. Ty dokáží pomocí tzv. hashe dané velikosti zredukovat zprávu neurčité délky na menší hashovací hodnotu v porovnání s původní zprávou.

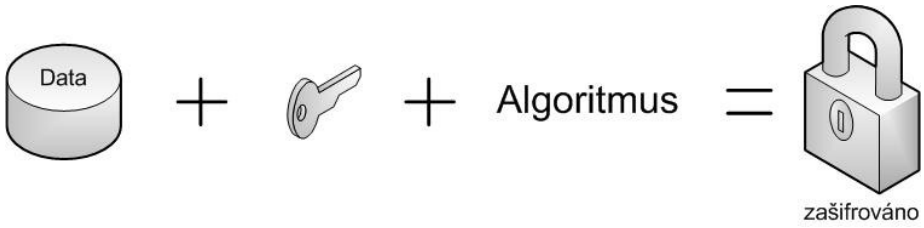
Podle Sisonsky (2010) je hashovací funkce zmenšená datová hodnota se ztrátou informací. Proto nelze dedukovat vůbec žádné informace o vstupních datech. A jelikož nelze výpočetně získat jakákoliv původní data.

MD4 (Message Digest 4) je starší hashovací funkcí vycházející z hashovací hodnoty o délce 128 bitů. *„Právě MD4 se používá ke kontrolním údajům o heslech vytvořených v systémech Windows NT, Windows XP/ Server 2003 a Windows Vista/ Server*

2008.(Sisonsky, s. 683, 2010)" MD5 (Message Digest 5) je v dnešní době nejznámější hashovací funkcí. Je nástupcem MD4 a taky je na této starší hashovací funkci založena spolu s SHA (Secure Hash Algorithm), který je prosazován americkým úřadem NSA (National Security Agency).

2.6.2 Asymetrické šifrování

Tyto algoritmy používají ke svému šifrování veřejný a soukromý klíč. Kde na základě veřejného klíče se data zašifrují, jak je zobrazeno na obrázku 2.5, a pomocí soukromého klíče se zase dešifrují. A právě na tomto principu pracují Diffie-Hellmanův šifrovací algoritmus a RSA šifrovací algoritmus, které jsou zmíněny v úvodu šifrování.



2.4 Šifrování pomocí veřejného klíče (vlastní)

Tento typ šifrování se používá například u digitálních podpisů, ale u nich se používá opačná technologie. Prostřednictvím soukromého klíče vznikne podpis a k jeho ověření se požívá veřejný klíč. Tyto klíče jsou párové, což znamená, že tyto klíče jsou navzájem propojené. Ale zjištění jednoho z klíčů za pomocí toho druhého je výpočetně nemožné.

Podle Sisonsky (2010) je algoritmus RSA založen na faktorizaci celých čísel, která se vytvářejí násobením velkých prvočísel, což je jeden z matematických problémů ve výpočetních úlohách asymetrického šifrovaní. *„Druhý typ problému, na který narazíme u algoritmu D-H-M, je založen na kalkulaci diskrétního logaritmu, který je derivován řešením rovnice* $gx = h$*, přičemž* g *a* h *jsou členy konečné cyklické grupy. (Sisonsky, s. 684, 2010)"*

2.6.3 Systém Kerberos

Sisonsky (2010) i Ministr (2013) tvrdí, že tento protokol je síťový autentizací systém, který je založen na principu symetrického šifrování a k tomu ještě používá třetí stranu, což umožňuje zjištění totožnosti obou stran, které mezi sebou navzájem komunikují. Z toho vyplívá, že se ve vztahu jedná o tři faktory:

- Klient
- Server

- Důvěryhodná autorita (KDC)

Podle Ministra (2013) je Kerberos založen na principu přidělování lístků, což jsou zakódované data pro ucházení se o službu na serveru. Sisonsky (2010) ve své knize uvádí, že samotný systém Kerberos prošel několika rozšířeními. Dnes tedy systém Kerberos zahrnuje autentizací algoritmy s asymetrickými klíči. V této podobě se Kerberos uplatňuje ve Windows Serveru 2008 nebo Windows Vistě.

V příloze – obrázky: Obrázek 1 se zobrazuje fungování autentizačního mechanismu Kerberos na Windows Serveru 2008 a vysvětluje postup fungování tohoto mechanismu.

2.6.4 Základní metody kódování informací bezdrátového přenosu

Podle Sosinského (2010) jsou tyto základní metody tři a to:

Pulzní modulace – je založen na binárním principu (zapnuto = logická jednička, vypnuto = logická 0).

Amplitudová modulace – používá k rozeznávání vln prahovou hodnotu. Pokud vlna této prahové hodnoty dosáhne, znamená to logickou jedničku, ale pokud je pod touto prahovou hodnotou, značí to logickou nulu.

Frekvenční modulace - je založená na proměnlivé frekvenci vln. Pokud frekvence přeroste danou prahovou hodnotu, znamená to logickou jedničku, pokud ale této hodnoty nedosáhne, značí to nulu.

2.7 Antivirová ochrana

V dnešní době antivirové programy prodělaly značný vývoj. Objevují se nové kvalitní nekomerční antivirové programy. Jejich rozdíl kvality oproti komerčním antivirovým programům není tak velký jaký byl v minulosti. Dnes se spíš jedná o cenu antivirového softwaru a také jeho dostupnosti, možnosti souhrnného užívání a velikost provozních nákladů.

2.7.1 Nasazení antivirového softwaru

Jednoúrovňové nasazení antivirového softwaru

Na pracovních stanicích se většinou uplatňuje jednoúrovňové nasazení antivirového softwaru, což je uskutečněno jen na jedné úrovni. Toto nasazení antivirového programu většinou nevyužívá centrální správu, tudíž tento program nechrání ostatní úrovně. Zde je nebezpečí, že daný vir bude zachycen až na pracovní stanici, což by mohl velký problém.

Víceúrovňové nasazení antivirového softwaru

Toto nasazení antivirového softwaru se uplatňuje na více úrovních. Podle Ludvíka a Štědroně (2008) jde převážně o pracovní (koncové) stanice, souborové servery a někdy i poštovní servery. Rozlišují se dva druhy centrální správy:

- **Dělená centrální správa** umožňuje centrálně spravovat z jednoho místa všechny stanice na jedné úrovni.
- **Komplexní centrální správa** umožňuje centrálně spravovat z jednoho místa všechny prvky.

Komplexní nasazení antivirového softwaru s komplexní centrální správou

Toto nasazení antivirového softwaru se provádí na všech úrovních. Podle Ludvíka a Štědroně (2008) se jedná o pracovní (koncové) stanice, souborové servery, poštovní servery a brány. Jako u víceúrovňového nasazení antivirového softwaru s komplexní centrální správou lze centrálně spravovat z jednoho místa spravovat všechny prvky. Toto nasazení antivirového softwaru od:

- **Jednoho výrobce**
  - Zde je nevýhoda závislost na tomto jediném výrobci, protože používá na všech úrovních totožnou virovou databázi.
- **Více výrobců**
  - Zde si musíme při nákupu dávat velký pozor na kompatibilitu všech prvků.
  - Výhodou je, že jednotlivý výrobci aktualizují svou databázi virů v jinou dobu. Pokaždé tuto databázi aktualizuje první někdo jiný, ale díky tomu se snižuje doba, kdy firma zůstává nechránění před novým virem. Tudíž se zvyšuje zabezpečení jisté firmy.

2.7.2 Viry

„Cohenova definice zní takto: „Virus je program, který je schopen infekce dalších programů a je schopen jejich modifikací zajistit, aby obsahovaly potenciálně se vyvíjející kopii jeho samotného.“(Szor, s. 38, 2006)“ Tato definice znázorňuje hlavní znaky viru, což je například jeho rozvoj.

Základní viry

Počítačoví červi

Tyto viry se převážně rozšiřují po síti nebo také e-mailem. Podle Szora (2006) se na vzdáleném počítači zahajují bez zjevného zásahu uživatele. Většinou se jedná o nezávislý program.

Logické bomby

Logická bomba je v podstatě naprogramovaná chyba programu. Je to například chyba v kódu, která zapříčiní vymazání dané aplikace z disku, jako součást zaštítění proti kopírování. Szor (2006) uvádí příklad na oblíbené hře Mosquitos na mobilních telefonech Nokia, která odesílala SMS zprávy na komerční linky.

Trojský kůň

Je to nejjednodušší druh škodlivého programu. Tento program se ‚tváří' důležitě, aby přiměl uživatele si tento program stáhnout a spustit ve svém počítači. Do tohoto programu hackeři připojí trojského koně. Pak jsou schopni zpětně tento program vypátrat a využít. Viry typu trojského koně známe dva:

- **Zadní vrátka (Back door)**
    - umožňuje vzdálený přístup k počítači,
    - zpravidla tento program po zahájení jeho činnosti zpřístupní síťový port na daném počítači.
- **Trojské koně s funkcí hledání hesel**
    - soustřeďují se na vyhledávání a následné expedování hesel útočníkovi,
    - většinou jsou sloučeny se skenováním stisků klávesnic.

Snímače stisku kláves

Jedná se o program nainstalovaný v počítači bez vědomí uživatele. Tento program pas snímá stisky kláves, z nichž zjišťuje důležitá data, jako jsou například jména, rodné čísla, PINy, hesla a čísla bankovních účtů atd.

2.8 Ochrana před pohromami a ochrana dat

2.8.1 Záložní zdroje

Jsou to zařízení, jenž chrání jiné zařízení před nebezpečným kolísáním elektrické energie nebo před přepětím a výpadkům elektřiny. Podle Ministra (2013) se dělí tyto prvky následovně:

Přepěťová ochrana je brána za nejlevnější bezpečnostní prvek, který by měl mít každý server, kritické pracovní stanice a důležité počítače zapojené do sítě. Tato minimální ochrana chrání zařízení v síti před kolísavým proudem, ale už je neochrání před poklesem napětí či samotným výpadkem proudu. Tyto zařízení málokdy vydrží více přepětí po sobě, tudíž po ochránění počítače musí být nahrazena novou.

Záložní zdroje energie (UPS) jsou dražší a lepší elektronické bezpečnostní zařízení, které je schopno při výpadku dodávat připojeným zařízením elektrickou energii po dobu 5 – 20 minut. Nejsou tedy určeny pro trvale dodávání proudu, ale poskytují energii jen na dobu pro řádné uložení rozpracovaných dat a následně pro náležité vypnutí příslušného zařízení. UPS se zapojují do elektrické zásuvky a na výstupu mají několik zásuvek pro chráněné zařízení. Při výpadku je pak uživatel varován, aby standardně uložil rozpracovanou práci a vypnul zařízení. Po opětovném zapnutí elektřiny se začne automaticky dobíjet.

Generátory jsou velice nákladná motorová zařízení vyrábějící elektřinu za použití určitého paliva (benzín, nafta, petrolej, atd.). Tyto zařízení jsou schopny napájet počítačovou síť po celou dobu výpadku.

2.8.2 Záloha dat

Podle Ministra (2013) můžou nastat hrozby (viz přílohy – obrázky: Příloha 3), které jsou zaměřené na disky, a data těchto disků mohou být náhle zničena, ztracena nebo nečitelná. Pokud se ale pravidelně uskutečňují zálohy, zabrání se úplné ztrátě těchto dat. Ideálně by se mělo zálohovat úplně všechno, ale to samozřejmě není z mnoha důvodů možné. Tudíž se zálohují hlavně prvotní dokumenty vytvořených v různých uživatelských aplikacích. Pravidlem je, že společnosti dělají dvě zálohy: jedna je umístěna ve firmě a druhá je umístěna na externím úložišti mimo prostory společnosti.

Jsou tři primární druhy zálohování:

1) **Úplné zálohování** – záloha veškerých dat na dané diskové jednotce bez ohledu na termín poslední uskutečněné zálohy.

2) **Rozdílové zálohování** – zálohování dat, která byla od posledního úplného zálohování změněna.
3) **Přírůstkové zálohování** – zálohování dat, která byla změněna od jakéhokoli posledního druhu zálohování.

Stále nejpoužívanějším zálohovacím mediem jsou páskové jednotka, ale ty jsou pomalu nahrazovány výměnnými disky ZIP nebo Jaz, dále také kompaktními disky CD-R a CD-RW a v neposlední radě i magneto-optickými disky.

2.8.3 Rezistence disku vůči chybám

Horák (2007) uvádí, že tato metoda vytváří z několika disků diskové pole vypadající na první pohled jako jeden disk. Významem diskových polí RAID však není zvýšení kapacity, nýbrž zvýšení bezpečnosti dat za pomocí redundance (nadbytečnosti) dat. Principy jednotlivých typů RAID jsou:

- **RAID 0 –** data jsou rozdělena na dva a více disků.
- **RAID 1 –** data jsou ukládány na dva disky. Čemuž se říká zrcadlení. Jeden disk je přesnou kopii (zrcadlem) toho druhého.
- **RAID 5 –** data i paritní informace jsou uloženy v pruzích na různých místech disku. Pokud jeden z disků selže, je vyměněn a jeho data jsou opravena za pomoci redundantních paritních informací.
- **RAID 10 –** tento typ RAID je spojením RAID 0 a RAID 1. Data jsou rozdělena mezi dva a více disky a každý RAID 0 má ještě sou přesnou kopii.

Podle Ministra (2013) mohou být RAID pole hardwarové i softwarové. Hardwarové řešení je ale rychlejší, spolehlivější a také dražší.

2.8.4 Rezistence serveru vůči chybám

Redundance je základem každé metody o ochraně před hrozbami. U serverů se jedná o podobu clusteringu neboli ‚seskupování'. Za pomoci těchto klastrů, je pak možno vidět skupiny serverů zapojených do sítě jako jeden server. A jestliže jeden z těchto serverů v klastru havaruje, ostatní za něj převezmou jeho úlohu.

3 Popis stávající počítačové sítě a jejího zabezpečení

Tato kapitola se zabývá identifikací aktiv umístěných ve firmě. Dále se zaobírá bližší specifikací stávajícího zabezpečení identifikovaných aktiv. Tato kapitola se primárně řídí českou technickou normou ISO/EIC 27005 z roku 2009, která blíže specifikuje postup analýzy rizik, ohodnocení těchto rizik a následné navržení opatření, která tato rizika minimalizují.

Popisovaná firma je společnost s ručením omezeným, která se zabývá správou městských bytů, správou bytů ve společenství vlastníků[1] a jinými realitními činnostmi. Tato realitní činnost zahrnuje kontrolu záloh za média v podobě tepla, teplé užitkové vody, studené vody, spotřeby elektrické energie za společné prostory domu a fondy oprav a v případě městských bytů i kontrolu nájemného. Všechna tato data jsou pak shromážděna spolu s osobními daty nájemníků a vlastníků bytů na databázovém serveru, kde jsou firmě k dispozici.

3.1 Rozvržení počítačové sítě ve firmě

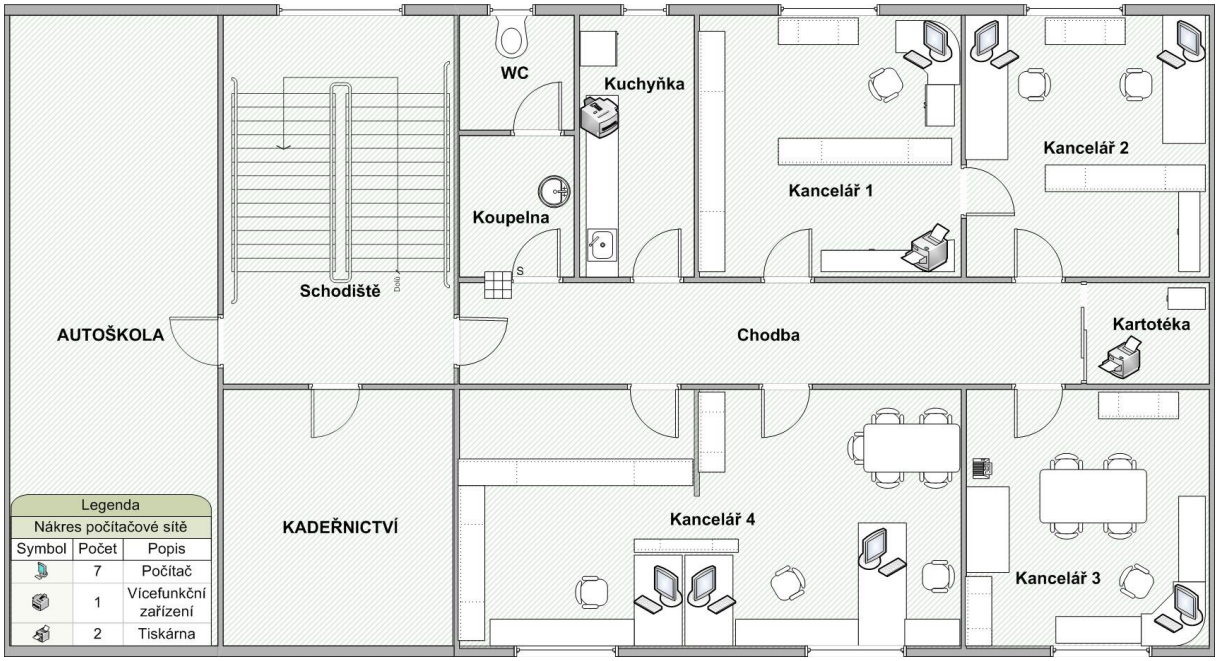
Počítačová síť této firmy je rozprostřena do tří pater budovy, kterou má firma ve svém vlastnictví. Do přízemí, zobrazeném v příloze – obrázky: Obrázek 8, které je pronajaté sousední bance a místnímu baru, počítačová síť nesahá.

Firemní počítačová síť sahá tedy od prvního patra, zobrazeném na obrázku 3.1, až po třetí patro umístěno pod střechou a fungující jako kancelář vlastníka a jednatele firmy (viz příloha – obrázky: Obrázek 9)

V těchto třech patrech se nacházejí hlavně kanceláře obsahující **koncové počítačové stanice** zapojené v typologii hvězda. S těmito koncovými počítači pracují zaměstnanci v rozhraní svých uživatelských účtů zařazených do určitých pracovních skupin, které pak mají odlišné oprávnění. Na těchto stanicích je nainstalován operační systém Windows XP Professional, ale pomalu se přechází na modernější operační systém Windows 7. Dále jsou na těchto počítačích nainstalovány aplikace a software, které jsou nezbytné pro práci dané firmy, například balíček Microsoft Office 2007, iDES[2], atd.

[1] Byty ve společenství vlastníků jsou umístěny v panelových domech nebo domech s více byty. Tyto byty mají ve svém vlastnictví vlastníci, kteří se sdružili nebo založili společenství vlastníků a správu nad svými byty přenechali dané firmě.

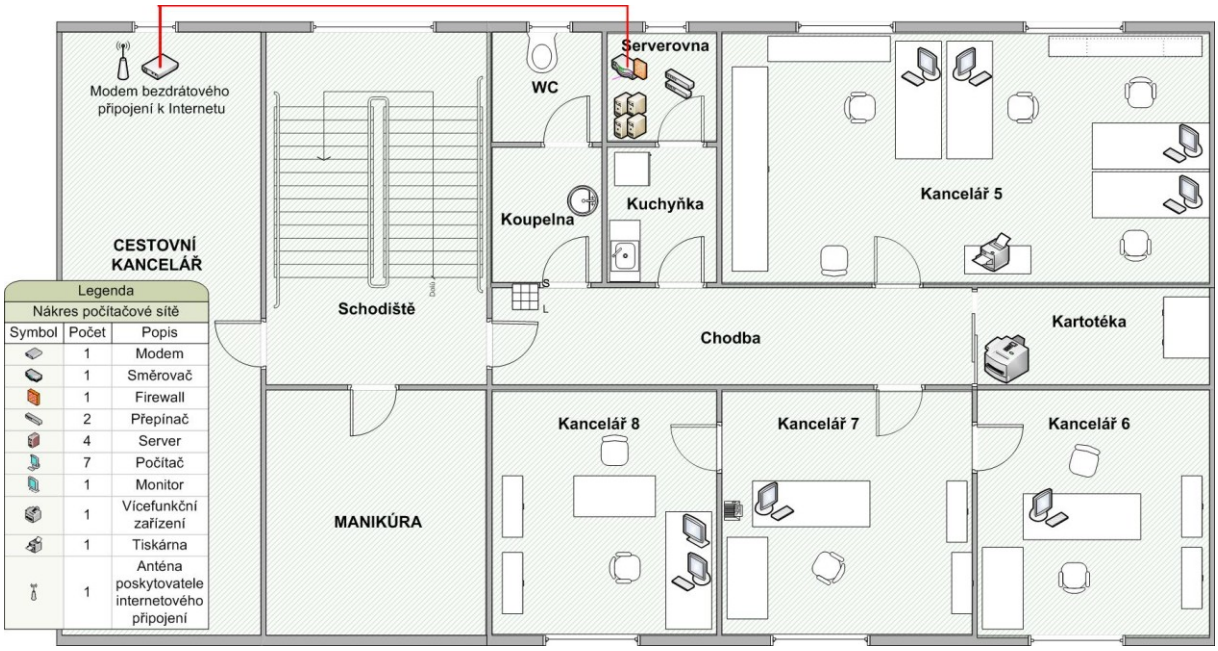
[2] Jedná se o program, který je určený pro správu domů. Svá data pak ukládá na SQL databázový server umístěný ve firmě.



3.1 Rozvržení počítačové sítě v 1. patře firmy (vlastní)

Serverovna

V serverovně jsou pak umístěny čtyři fyzické servery (formulářový, poštovní, databázový a zálohovací server), tři switche (switch 1 a switch 2, což jsou dva switche propojené tak, aby vypadaly jako jeden), firewall s přidanou funkcí směrovače a patch panel.



3.2 Rozvržení počítačové sítě v 2. patře firmy (vlastní)

Hardwarový firewall typu Zyxel Zywall 70 slouží nejen jako ochranná zeď, která zaručuje bezpečí vnitřní síti firmy, ale také jako router. Jedná se tedy o zařízení vše v jednom. Je to poměrně využívaný typ zařízení mezi malými a středními firmami. Zywall 70 spojuje firewallové povinnosti NAT a SPI, dále také obsahuje bezpečnostní protokol IPsec pro VPN. Umožňuje také filtrovat obsahy webových stránek. Jako firewallová brána má od počátku své základní zásady, které zahrnují připojení LAN, WAN a DMZ. Samozřejmě je možné nastavit i vlastní zásady. Jeho nevýhodou je však nedostatečný antivir a antispam.

Tento hardwarový firewall má zakomponovaný DHCP server, kde je možné nastavit dynamicky IP adresy pro jednotlivé servery, ale tato funkce je ve firmě nevyužívaná.

Každý server i počítač mají své staticky definované IP adresy nastavené přímo na samotné stanici. Servery však dostaly své IP adresy od samotného poskytovatele internetového připojení. IP adresy ve vnitřní síti jsou definovány ve tvaru 192.168.0. XXX.

Formulářový server je fyzický server zapojený mimo vnitřní síť firmy. Tomto server využívá operační systém Windows server 2008 R2 Standard od firmy Microsoft. Jak už poukazuje název tohoto serveru, slouží pro tvorbu a ukládání formulářů, které jsou nezbytné pro fungování firmy. Dále je používán jako takzvaný ‚generátor sestav'. Což znamená, že z databáze firmy jsou vyexportované data, jako CSV soubor, který se pak načte do formuláře. Výsledný soubor je pak uložen ve formátu PDF. Tato nadstavba operačního systému Windows server 2008 R2 Standard je poskytována firmou Software602, jako 602XML řešení. Jedná se o takzvané ‚elektronické inteligentní formuláře'.

Poštovní server je jako formulářový server zapojený mimo vnitřní síť firmy. Také se jedná o fyzický server, na kterém je nainstalován Linuxový serverový operační systém Debian GNU/Linux 4.0. Na tomto fyzickém serveru je pak nainstalován VMware, což je software, pomocí něhož jsou spouštěny virtuální servery, jako je například níže uvedený webový server, souborový server a třetí virtuální server, který firma plánuje v brzké době vytvořit.

Webový server využívá pro svůj chod, stejně jako výše uvedený poštovní server, univerzální Linuxový operační systém Debian GNU/Linux 4.0. Jedná se o virtuální server ve firmě, který běží v programu VMware. Tento server je pak využíván pro podporu firemních webových stránek, které jsou zhotoveny pomocí aplikace Joomla 2.5, což je podle Českého Webhostingu jeden z nejvyhledávanějších redakčních systémů pro tvorbu webových stránek. Pod další činnosti tohoto redakčního systému spadá i administrace těchto stránek, která vede k jednoduché aktualizaci dat na stránkách. Joomla 2.5 má tu výhodu, že je poskytována

v českém jazyce zdarma a lze ji rozšířit o balíčky, které zahrnují elektronický obchod, diskusní fóra nebo fotografie.

Databázový server je dalším fyzickým serverem ve firmě. V operačním systému Windows server 2008 R2 Standard od firmy Microsoft je nainstalován Microsoft SQL server 2012 pro správu samotných databází.

Souborový server jak už z jeho názvu vyplývá, poskytuje firmě úložiště pro veškeré soubory a adresáře. Přístup k těmto souborům je pak definován v pracovních skupinách. Tento server je stejně jako webový server virtuální a spolu s ním taky funguje ve VMware s Linuxovým operačním systémem Debian GNU/Linux 4.0.

Zálohovací server je posledním fyzickým serverem v dané firmě, který používá Windows server 2008 R2 Standard. Tento server pro zabezpečení zálohy veškerých dat firmy používá metodu zálohování D2D(2T) s pomocí RAID polí typu RAID 5 vytvořených ze čtyř fyzických disků.

Switch 1 je zařízení od firmy Zyxell. Do něj jsou zapojeny formulářový a poštovní server. Důvod tohoto zapojení spočívá ve snaze ochránit vnitřní síť vytvořením vnějšího úseku pro tyto servery, které komunikují s Internetem.

Switch 2 se skládá ze dvou větších switch panelů Zyxel ES1100-24E propojených mezi sebou a navenek se tvářící, jako jeden switch panel. Do tohoto switche jsou přes patch panel napojeny jednotlivé počítače a servery zapojené ve vnitřní počítačové síti.

Patch panel slouží ve firmě výhradně jen za účelem snadného a rychlého přizpůsobení vedení linek při přesunu systémů. Pro vedení linek je požit standardní síťové kabely (kroucená dvojlinka) s koncovkou RJ-45.

3.2 Použité antivirové zabezpečení

Firma používá komplexní antivirový systém na všech úrovních od poskytovatele ESET v podobě balíčku ESET Secure Business, který zahrnuje ochranu na pracovních stanicích, mobilní zařízení, souborových serverech, poštovních serverech a v neposlední řadě i firewally a antispamy. Na tento balíček služeb firma každé dva roky prodlužuje licenci, která stojí přibližně 18 000 Kč.

Zabezpečení stanic zahrnuje antivirovou a antispywarovou ochranu, která odstraňuje hrozby v podobě virů, červů a spywaru. Dále umožňuje formulovat pravidla pro registry, procesy, aplikace a soubory. Samozřejmostí je automatická kontrola externích medií a další.

U **souborových serverů** kromě antivirové a antispywarové ochrany, která zahrnuje i Modul Self-Defense[3], dále také multiplatformovou ochranu. Tato ochrana omezuje rozšiřování, potažmo likviduje škodlivé kódy na jiných platformách než je Windows. Například Linux, který je ve firmě použit.

Zajištění bezproblémového provozu je další funkcí balíčku ESET Secure Business na úrovni souborového serveru. Což zahrnuje určení totožnosti uživatelských účtů, které se pokoušejí o proniknutí. Dále pak zajišťují odinstalace heslem.

Zabezpečení **poštovního serveru** podle ESET (2012) obsahuje kromě antiviru a antispywaru, což mimo jiné i filtruje emailové hrozby, která by se v dané firmě mohla naskytnout, také antispam likvidující nežádané zprávy a poštu obsahující tzv. phishing[4]. Dále tato ochrana obsahuje bezproblémový provoz, protokoly a statistiky, které sledují výkon serveru a tzv. Greylisting protokol. Tento protokol zahrnuje data o odesílateli, příjemci, provedené akci a informace o ukončení.

Tento balíček dále obsahuje zabezpečení mobilních zařízení, která se ve firmě nevyužívá, a firewallu.

3.3 Zabezpečení místnosti

Místnosti jsou zabezpečeny pomocí různých zámků. Od těchto zámků mají klíče jen zaměstnanci, kteří v dané kanceláři pracují, vlastník – jednatel firmy a nakonec IT specialista firmy, který má pod správou veškeré počítače v dané firmě. Pak také ve firmě používají bezpečnostního zařízení na principu číselného kódu nainstalovaného v každém patře. Toto zařízení je v případě vloupání schopno přivolat příslušnou pomoc do dvou minut. K tomuto bezpečnostnímu zařízení má každý zaměstnanec firmy svůj vlastní kód.

Serverovna je umístěna ve druhém patře, jak je znázorněno na obrázku 3.2, za dvojitým zámkem (jeden zámek na dveřích od kuchyňky a druhý u dveří od serverovny). Od

[3] Modul Self-Defense brání škodlivému kódu a neautorizovaným uživatelům vypnout antivirovou ochranu.

[4] E-mailová zpráva vypadající jako důvěryhodná, ale má za úkol zjišťovat soukromé informace a hesla uživatele e-mailu. Někdy taková zpráva žádá určitou sumu peněz.

samotné serverovny pak mají klíče jen dva lidé (IT specialista a vlastník – jednatel firmy). Ventilační okno nemá mříže a je od země oddělené sedmi metry.

3.4 Použité serverové a jiné operační systémy

3.4.1 Servery

Windows Server 2008 R2 Standard

Jedná se o jeden z nejpokročilejší operační systém pro servery od firmy Microsoft. Je hlavně určen pro novou generaci sítí, aplikací a webových služeb. Za pomocí tohoto operačního systému je firma schopna spravovat data z vyspělého uživatelského prostředí, které zabezpečuje síťovou infrastrukturu. Ve firmě je tento operační systém využíván zejména na databázovém serveru, formulářovém serveru a zálohovacím serveru.

Debian GNU/Linux 4.0

Operační systém Debian požívá jádro od firmy Linux. Tento serverový operační systém má lepší podporu šifrování než jeho předchozí verze. Také je tato verze vylepšena ze strany bezpečnosti a efektivnosti, což zmiňuje Debian (2007).

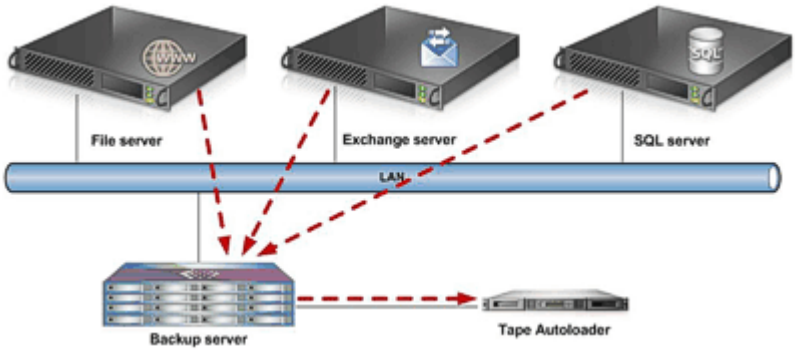
3.4.2 Stanice

Ve firmě se používá na stanicích hlavně operační systém Windows XP Professional, ale v poslední době se pomalu přestupuje na operační systém Windows 7 rovněž od firmy Microsoft. Firma se rozhodla právě pro Windows 7, kvůli jeho vylepšení a rozšíření oproti zastaralému, ale stále celkem dostačujícímu operačnímu systému Windows XP Professional. Hlavní rozdíly těchto dvou používaných operačních systému jsou uvedeny v příloze – tabulky: Tabulka 4.

3.5 Zálohování dat na fyzických serverech pomocí metody D2D(2T)

Jedná se o metodu, která je složena ze dvou fází. První fází této metody je zálohování dat do diskového pole a druhou fází je klonování této zálohy na vysokokapacitní, přepisovatelné páskové záznamové médium. Tato metoda řeší mnoho nedostatků vyskytujících se u klasické metody zálohování, jako jsou například zkrácení zálohovacího okna, použití celé rychlostní kapacity zálohovací mechaniky a také se účastní na duplicitě dat a tím přispívá k její zvýšené bezpečnosti.

Dále jsou zálohovaná data stále připojena k diskům, tudíž jsou stále firmě k dispozici. Prostřednictvím čehož lze data obnovit ve velmi krátkém časovém intervalu. Také není nutné při zálohování na disky řídit a uchovávat páskové zálohovací media externě (viz obrázek 3.3).



3.3 Zálohovací systém (Zálohování dat, 2013)

K zálohování dat na disky v zálohovacím (Beckup) serveru je používán RAID 5 se čtyřmi disky. Principem tohoto rozložení dat na zálohovací disky je, že se mezi tyto disky data rovnoměrně rozloží. ‚Přebytečná' stejná data jsou taktéž rozložena na všechny čtyři disky. Proto, když jeden z disků havaruje, je možné ho vyměnit a jeho data jsou pak zrekonstruována pomocí stejných, opakovaných údajů.

Tento typ RAIDu je ve firmě používán, protože zvyšuje výkon při čtení z disku. Dále také s ohledem na výhodu výše zmíněná snadnost vyměnění disku s tím, že data se dopočítají a zrekonstruují. A nakonec je pro firmu výhodou i to, že opakující se data nezabírají tak velkou část disku, čímž se nemusí zvyšovat kapacita těchto disků. Nevýhodou tohoto typu RAIDu je nezbytnost minimálně tří pevných disků, ale to firmě nevadí, kvůli existenci čtyř fyzických disků, které museli s ohledem na velké množství dat, které se musí zálohovat, ve firmě pořídit.

Tyto zálohy se provádějí každý den a zálohy jsou uloženy na třech různých místech: na výše zmiňovaných čtyřech discích zálohovacího serveru, na páskových médiích vytvořených daným zálohovacím serverem a pak existuje záloha, která není umístěna přímo v budově firmy, ale na externím úložišti firmy, které z důvodu bezpečnosti firma nesmí přesněji specifikovat.

Dále firma zálohuje data ve formulářových podobách v podobě tištěných dokumentů, které jsou dále roztřízeny do jednotlivých oddílů podle spravovaných domů, dále podle bytů a jména vlastníka či nájemníka. Tyto oddíly jsou pak zakládány do kartoték, které jsou umístěny v jednotlivých kancelářích, aby byly pracovníkům po ruce. Kopie těchto dokumentů pak mají i jednotlivý vlastníci či nájemníci bytových jednotek.

3.5.1 Virtuální servery

U virtuálních serverů, na kterých běží souborový server a webový server, je záloha dat jednoduší než jak tomu je u fyzických serverů. Každý ze dvou virtuálních serverů běžící v programu VMware a má svůj vlastní klon, který je každý den aktualizován. Pokud tedy nějaký ze serverů zhavaruje, jednoduše ho nahradí jeho dvojče, které není v chodu, pokud je předešlý server v chodu.

3.6 Zabezpečení serverů a dalších systémů před výpadky elektřiny

Každý server, který je zapojený do sítě firmy, je chráněn samostatným záložním zdrojem (UPS). Jedná se o Smart-UPS SMT750l od firmy APC. Tyto záložní zdroje zahrnuji i přepěťovou ochranu, která chrání servery před výkyvy elektrického proudu. Dále poskytuje i kvalitní filtraci šumu a automatickou regulaci napětí. Také šetří náklady na spotřebu energie a chlazení.

Tyto záložní zdroje ale nevydrží servery napájet po celou dobu výpadku elektrického proudu. Proto každý server se svým záložním zdrojem komunikuje. Dojde-li pak k neplánovanému výpadku elektřiny, UPS vyzve server, který má na starosti, aby regulérně uložil veškerá upravovaná data a následně se korektně sám vypnul.

Samostatný záložní zdroj má i bezpečnostní alarm zabezpečující prostory (kanceláře) firmy.

Ostatní počítačová zařízení mají pouze přepěťovou ochranu, protože používaná data jsou uloženy na discích serverů a ne na discích využívaných stanic, které se pro tyto data ‚natahují' do uvedených serverových disků. Tudíž je to podle analyzované firmy nesmyslné zapojovat do dalších nákladných záložních zdrojů i počítačové stanice uživatelů.

3.7 Uživatelské účty, hesla a skupiny

Uživatelské účty jsou nastaveny na míru jednotlivým pracovníkům zařazených v pracovních skupinách. Jednotlivé pracovní skupiny mají nastaveny odlišná oprávnění k manipulaci s daty. Tyto pracovní skupiny mají přístup jen na svá příslušná místa v síti. Některým z nich je dokonce povolena práce s flash disky. Firemní data jsou v podstatě jen databázové tabulky a bez ‚runtime' se k nim kromě administrátora nikdo nedostane. Tudíž lze ‚runtime' chápat jako program nebo knihovnu, která je vestavěná do programu. Tento program má pak funkci pro vsup, výstup a správu paměti.

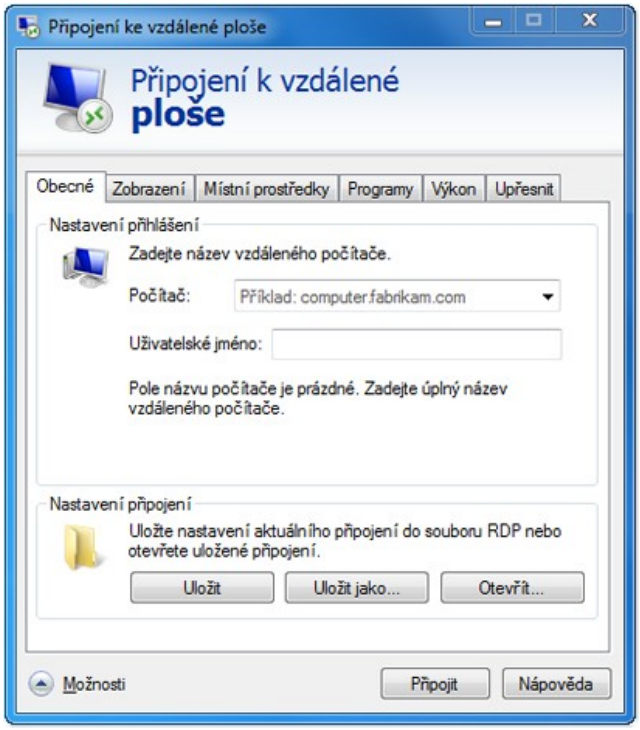
Každý zaměstnanec má ke svému uživatelskému účtu heslo, které je založeno na principu matematické kombinace čísel, písmen a znaků. ‚Síla' hesel je kontrolována správcem sítě (IT specialistou) a v případě nedostatečně silného hesla je pak heslo aktualizováno do silnější formy.

Například kdysi bylo ve firmě možné mít heslo ‚Prosím'. Teď tahle podoba hesla nepřipadá v úvahu.

Dále je ve firmě dohlíženo na to, aby se jednotlivá hesla aktualizovala minimálně co dva roky. Pokud nedojde ke zvláštním událostem, jako je například změna v systému pracovních pozic. V tomto případě se mění hesla podle potřeby.

3.8 Připojení externích zařízení

IP adresa u notebooku je staticky nastavena stejně jako u ostatních zařízení ve firmě přímo na stanici. Pak je tato IP adresa uvedena v hranovém firewallu v seznamu IP adres, kterým je umožněn přístup k vnitřní počítačové síti. A za pomocí nastavení **vzdálené plochy** počítače, jež je umožněno v operačních systémech Windows 7 (viz obrázek 3.4), je pak možno do této sítě přistupovat z externího místa.



3.4 Připojení ke vzdálené ploše ve Windows 7 (Připojení ke vzdálené ploše, 2013)

Toto zapojení je nastaveno pouze u notebooku vlastníka - jednatele firmy, kvůli nutnosti flexibility tohoto notebooku a dat, které jsou na něm uloženy.

Ve firewallu je také definován **přístup do firemní databáze** přes protokol HTTPS. Tento protokol má výhodu implementovaného šifrování SSL, které zašifruje data při přenosu po firemní síti, přitom samotné toto šifrování i s bezpečnostním protokolem HTTPS běží na aplikační vrstvě modelu OSI (viz přílohy – obrázek: Obrázek 2).

Tento přístup umožňuje pořizovat data, prohlížet tyto data a vytvářet z nich výstupní sestavy, které jsou dále k dispozici. A veškerá tato manipulace s daty je zašifrována pomoci asymetrického šifrování v podobě SSL.

3.9 Připojení k internetu

Společnost, od které se daná firma rozhodla odebírat internetové připojení, je v daném městě jedna z nejrozšířenějších poskytovatelů internetového připojení a je také jedna z nejspolehlivějších. Firma s tímto poskytovatelem zatím neměla žádné potíže. Tento poskytovatel však nepoužívá k připojení k internetu jednotlivých firem nebo domácností optické kabely, které by zabezpečily vysokorychlostní přenos, ale bezdrátové připojení. Díky tomu je poskytovatel schopen rychle reagovat na požadavky nebo stížnosti dané firmy či jiných jejich klientů.

Internet je do firmy přiveden pomocí UTP kabelu kategorie 5E[5] tažené po fasádě firemní budovy. Firma přijímá internetové připojení přes modem sousední cestovní kanceláře, která je v pronájmu v budově dané firmy a má svou anténu od tohoto poskytovatele, což je zřejmé z obrázku 3.2.

[5] Jedná se o výkonnostní kategorizaci. Kategorie 5E je nejrozšířenější kabeláž, která je schopna přenosové rychlosti až 1Gb/s.

4 Analýza a návrh bezpečnosti, zhodnocení řešení

Při analýze a návrhu bezpečnosti počítačové sítě v kategorii malé až střední firmy, do které spadá i daná firma, se vycházelo z pravidel pro zabezpečení takové sítě a z české technické normy ISO/IEC 27005 z roku 2009. Tato bezpečnostní pravidla a normy pomáhají předcházet útokům na firemní síť a také předcházet ztrátě nebo poškození důležitých dat v dané firmě.

4.1 Analýza rizik

Analýza rizik dané firmy se skládá z několika bodů. Body jako jsou identifikace aktiv a identifikace stávajícího opatření vybrané firmy jsou rozebrány v předchozí kapitole. Dalšími body jsou identifikace zranitelností, hrozeb a jejich následků, jež mají na firemní počítačovou síť, budou rozebrány následovně.

4.1.1 Identifikace zranitelností

Definované zranitelnosti nemusí působit škodu dané firmě jako takové. První je zapotřebí hrozby, která tuto zranitelnost využije. Z čehož vyplívá, že pokud bude ve firmě identifikována nějaká zranitelnost, která nebude mít hrozbu, na tuto zranitelnost firma nemusí uplatňovat žádné opatření, ale měla by jí nadále monitorovat. Zranitelnosti v dané firmě byly identifikovány pomocí obecně známých zranitelností v české technické normě ISO 27005 z roku 2009 (viz příloha – obrázky: Příloha 5, 6, 7).

Identifikace zranitelností z pohledu hardwaru

V dané firmě jsou zranitelnosti z pohledu hardwaru hlavně v podobě citlivosti daného hardwaru jak na vlhkost či prach, tak na citlivost zněm napětí nebo teplotu. Teplota je velkou zranitelností hlavně u serverů, protože ty pracují na vysoký výkon a mohly by se přehřát. Z toho důvodu by měla být serverovna dobře větraná. Ve firmě jsou proti této zranitelnosti vybaveny velkými okny v každé pracovně, kde se nalézá počítačové zařízení, přičemž servrovna má ještě ventilační průduch.

Další hardwarovou zranitelností je nechráněné uskladnění, které by mělo v dané firmě za důsledek krádeže médií nebo dokumentů nebo jejich úmyslné poškození. Ve firmě je tato zranitelnost zabezpečena alarmem na každém patře firmy a personálním pravidlem zamykat kancelář, při každém delším odchodu z firemních prostor, jako je například odchod do banky, pojišťovny, schůzka s klienty, dohled na opravy domů nebo i oběd, atd.

Ale serverovnu chrání jen dvojité dveře se zámky a alarm. V serverovně je pak velké okno, které je sice ve druhém patře, ale také je těsně pod střechou a dalo by se rozbít a zcizit zařízení umístěná v této místnosti. Stačilo by dát na toto okno nějakou fyzickou ochranu, například v podobě mříže nebo vnější pevné kovové stínidlo.

Identifikace zranitelností z pohledu softwaru

Mezi softwarové zranitelnosti se řadí hlavně problémy se softwarem jako je jeho přetížení, kolaps nebo nesprávné používaní, což má v důsledku odezvu hlavně na datech firmy. Těmto zranitelnostem se dá zabránit pravidelnými kontrolami systému, pravidelnou aktualizací softwarového vybavení firmy, potažmo školením zaměstnanců.

Další zranitelností tohoto sektoru v dané firmě je neodhlášení se z uživatelského účtu při odchodu, což by mohlo vést ke zneužití oprávnění. Tato zranitelnost je ošetřena dalším personálním pravidlem.

Nebo ze strany správce sítě firmy, že špatně nadefinuje přístupová práva jednotlivým uživatelům či pracovním skupinám nebo špatně nadefinuje hesla či nepřímo vystaví nebezpečí tabulky s hesly a to by mohlo ohrozit firmu z pohledu falšování práv.

Identifikace zranitelností z pohledu sítě

V této kategorii lze počítat se dvěma zranitelnostmi firmy a to nedostatečnou bezpečnostní architekturou sítě a s tím spojené nedostatečné řízení sítě, což by mohlo zapříčinit přetížení informačního systému.

Identifikace zranitelností z pohledu zaměstnanců

S personálními zranitelnostmi se musí potýkat každá firma nevyjímaje tuto analyzovanou firmu. Může se jednat, jak o nedostatečné bezpečnostní školení ze kterého vyplývá chybné použití zařízení či dokumentace, nebo nedostatek povědomí o bezpečnosti jako takové v podobě bezpečnostních pravidel a řádů firmy. Dále je zranitelností i nedostatek kontrolních mechanismů, které by mohlo vést k nezákonnému zpracovávání dat.

Identifikace zranitelností z pohledu lokality

Budova, ve které firma sídlí, se nachází u rušné hlavní cesty, mezi náměstím a sídlištěm. Budova je rozsáhlý komplex, čímž je myšleno několik budov postavených těsně u sebe s jednou nebo více sdílených stěn. V daném komplexu se nachází kromě kancelářských

prostor v budově firmy (mimo danou firmu v budově sídlí i autoškola, kadeřnictví, manikúra, cestovní kancelář, pronajímaný byt a kanceláře níže uvedené banky) obchodní centrum, železářství, optika, bar, kavárna a pobočka Československé obchodní banky, která prodloužila své pracovní plochy i do budovy firmy s tím, že dveře ve vstupních prostorech v přízemí (viz příloha – obrázky: Obrázek 8) byly zazděny. Nejstřeženějším objektem tohoto komplexu je pobočka banky, ale bohužel se vchod nachází na rohu komplexu a tudíž její kamerový systém nezabírá vchod do firmy.

Do budovy se vchází dřevěnými prosklenými dveřmi nebo zadními dveřmi, za nimiž je výkladová zóna pro dodavatele chráněna branou.

Do prostor s kancelářemi firmy se vchází dřevěnými dveřmi s protipožární výztuhou. Za těmito dveřmi jsou pak samotné kanceláře, které jsou chráněné systémem zámků a bezpečnostním alarmem. Bezpečností alarm se deaktivuje při zadání číselného kódu. Tato ochrana je shledávána dostačující vzhledem k tomu, že se jedná o malou firmu.

Identifikace zranitelností z pohledu organizace

V této kategorii zranitelností se jedná hlavně o nedostatky ze strany managementu vybrané firmy. Zvláště nedostatky ve formálních postupech či definování povinností nebo nedostatečné dodržování pravidel. Tyto zranitelnosti pak vrcholí chybným užíváním, odepření činnosti, zneužití oprávnění nebo také poškozením dat a chybám údržby systému.

4.1.2 Identifikace hrozeb

Při identifikaci hrozeb je nutné definovat a nalézt každou možnou hrozbu, ať je jakéhokoli typu nebo z jakéhokoli vnitřního či vnějšího prostředí. Tyto hrozby z velké části odpovídají nalezeným zranitelnostem, které jsou předem definovány.

Při identifikaci hrozeb by se mělo vycházet z předchozí analýzy rizik v dané firmě, bohužel takový dokument ve firmě není k dispozici. Tudíž je možné vycházet z obecného seznamu hrozeb, který ve svých přílohách přikládá i výše zmíněná norma ISO 27005 (viz příloha – obrázky: Obrázek 3 a Obrázek 4).

Fyzické poškození

Hrozba požáru je reálným rizikem pro každou firma. Požár může vzniknout z nedbalostních nebo nahodilých příčin, jako je zkrat vedení, zásuvek nebo prodlužovacích kabelů. Těmto příčinám lze zabránit pomocí pravidelných kontrol. Nebo z úmyslných příčin,

které jsou celkem reálné díky přítomnosti baru v přízemních prostorách. Této příčině však zabránit nelze. Je ale možné za podpory detektorů kouře minimalizovat škody.

Poškození vodou by v této firmě také mohlo nastat. Například serverovna je umístěna do prostoru vedle kuchyňky pro personál a podobné zařízení je umístěno i o patro výš přímo nad touto serverovou. Pokud by došlo k vytopení a voda by se dostala až do serverovny a mohlo by dojít ke zkratování serverů a dalšího zařízení, které se v této místnosti nachází. Tomu by se dalo vyhnout za pomoci například serverových skříní.

Zničení zařízení nebo médií by mohlo nastat buďto náhodně a to nedbalým nebo neopatrným zacházení se zařízením, což by mohlo skončit ztrátou aktuálních dat, nemluvě o škodě na zařízeních či médiích. Nebo úmyslně, co by mohl provést cizí člověk s vědomým úmyslem poškodit firmu nebo zaměstnanec s tímtéž úmyslem. Tomu lze zabránit dobrým bezpečnostním systémem pro ochranu prostor a poučení zaměstnanců o manipulaci s takovými zařízeními potažmo o finančních a právních následcích úmyslného či nechtěného zničení podobných zařízení a datových médií.

Prach, který se dostane do jednotlivých zařízení, jako jsou například serverové stanice nebo také počítače jednotlivých uživatelů, by mohl zapříčinit nadměrné přehřívání těchto zařízení. A jelikož většina procesorů má nastavenou maximální teplotu při, které se musí vypnout, je možné že se při značném přehřátí stanice vypne bez uložení rozpracovaných dat. Což způsobí nechtěnou ztrátu těchto dat. Jestli-že se pak toto nadměrné přehřívání opakuje, roste šance zničení součástí zapojených ve stanici (například základní deska, síťová karta, grafická karta a jiné). Této hrozbě se dá vyhnout pomocí pravidelného čištění větracích zařízení v přístrojích nebo rovnou čištění vnitřních komponent jednotlivých zařízení.

Toto riziko se často vyskytuje u notebooků. Díky jejich schopnosti přenosnosti a možnosti tato zařízení použít téměř na každém místě je hrozba zanesení prachem vyšší.

Přírodní události

V místní lokalitě je pro danou firmu jedinou přírodní hrozbou **meteorologický jev**, což znamená buďto vichřici, která by například poškodila anténu nebo jinak ohrozí aktiva firmy, nebo tato hrozba může přijít v podobě blesku, který je schopen narušit přívod energie či ‚vyhodit' jističe. Meteorologické jevy bohužel nejdou předvídat dopředu, ale mohou se přijmout opatření proti důsledkům této hrozby v podobě UPS, které firma využívá na klíčových zařízeních, jiné přepěťové ochrany a jiné.

Ztráta základních služeb

Výpadek proudu je ohrožením, které závisí na třetí osobě a je časově neodhadnutelná. Hrozí vypnutí systémů sítě analyzované firmy. Představuje velké ohrožení dat a u disků, které běží roky bez přestání, hrozí, že při znovuspuštění by mohl vyhlásit chybu. Minimalizovat tuto hrozbu můžeme pomocí UPS popřípadě pomocí generátorů.

Výpadek Internetového připojení je nepředvídatelná hrozba. Není to bohužel jediná stránka této hrozby. Jedná se také o to, že této hrozbě nemůžeme nijak zabránit. Avšak firma tuto hrozbu zmenšila, když si vybrala jednoho z nejspolehlivějších poskytovatelů Internetového připojení ve městě, kde firma sídlí.

Tato hrozba může být i úmyslná a to v případě když firmě někdo přestřihne nebo vypojí drát tažený z modemu sousední firmy po fasádě budovy.

Ohrožení informací

Tento typ ohrožení přichází hlavně od lidského faktoru a málokdy se jedná o neúmyslné (náhodné) činnosti. Pokud se jedná o virové napadení, značí to úspěšný průnik hackera. A **úspěšné napadení hackerem** je hrozbou, kterou by se měla zabývat každá firma pracující s financemi a osobními údaji svých klientů. Dosud se tato hrozba v dané firmě nevyplnila. Ochranou před tímto útokem jsou bezpečnostní hardware, bezpečnostní systémy a různé aplikace.

Dalšími hrozbami tohoto typu je například **vzdálená špionáž**, která vypadá podobně, jako klasická průmyslová špionáž konkurenční firmy (viz příloha – obrázky: Obrázek 4). Nebo **vyzrazení vnitřních informací firmy, odhalení pozice** jsou rizika, které hrozí zejména ze strany zaměstnanců. Proto je potřeba zaměstnance dobře informovat o hrozících finančních respektive právních postizích při přistižení u takového úniku informací.

Následující hrozbou je **krádež zařízení** a to je spíš záležitost lidí z externího prostředí. Proti této hrozbě je možné firmu chránit pomocí soustavy klíčů a bezpečnostního zařízení nebo také zabezpečení oken v nižších patrech firemní budovy.

Technické selhání

V analyzované firmě se hlavně jedná o **selhání zařízení nebo chybné fungování zařízení.** Většinou to jsou nahodilé hrozby, pokud se nejedná o virovou infekci systému.

Muže se také jednat o přetížení daného zařízení z důvodu zastaralých součástí, které ‚přesluhují' nebo zakomponování nových součástí, které ale nejsou kompatibilní se stávajícím zařízeními.

Dalším technickým selháním je této firmě **přetížení informačního systému**. Je možné, že při takovém přetížení nastane v operačních systémech Windows nebo i Linux systémová chyba, která pak nejde jinak opravit než restartováním. Této fatální chybě se přezdívá modrá obrazovka smrti. V důsledku restartování počítače může dojít ke ztrátě dat, protože se data v počítači korektně neuložila a následně se počítač regulérně nevypl.

Následně se mezi technické selhání počítá i **chyba v údržbě**. Jelikož žádný lidský zdroj ve firmě ani nikde jinde není neomylný, je možné něco opomenout nebo neúmyslně zanedbat, což má za následek zrovna technické selhání zařízení. K chybě údržby by mohlo dojít i úmyslně ze strany interního zaměstnance. Tudíž je potřeba zaměstnance dobře informovat o správné údržbě svých přidělených zařízení a také o hrozících finančních respektive právních postizích pokud se nebudou řídit danými pravidly.

Některé z hrozeb technického selhání jsou úzce spjaty s hrozbami fyzického poškození a snadno se mezi sebou zaměňují. Proto pro rozlišení těchto hrozeb byla použita norma ISO 27 005 z roku 2009 (viz přílohy – obrázky: Obrázek 3).

Neoprávněné činnosti

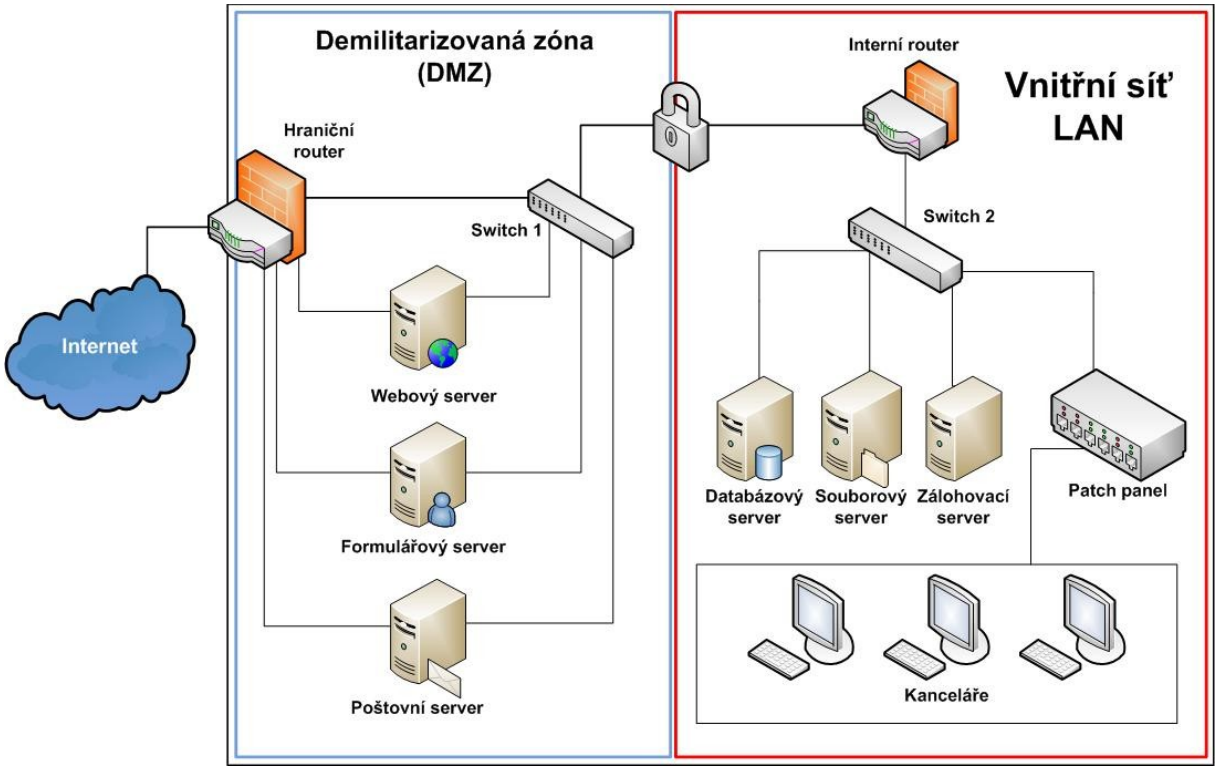
Mezi tyto činnosti se řadí **poškození dat**. Jedná se o data, která jsou poškozena úmyslně i neúmyslně. Třeba v důsledku používání špatných dat v nějakém aplikačním programu firmy. Tomu lze zabránit stejně jako například chybě v údržbě, informováním nebo školením pracovníků a informováním o dodatečných postizích.

Ohrožení funkčnosti

Tento poslední typ hrozby obsahuje **chybu v používání**. Což je bráno jako náhodné ohrožení ze strany lidského faktoru vnitřního prostředí firmy. Opět se tomu dá předcházet školením.

V neposlední řadě je nutné zmínit **nedostatek personálu**. Personál může onemocnět nebo odejít za lepším. Této hrozbě nelze nijak předvídat, lze s ní pouze počítat.

4.2 Návrh bezpečnostního řešení



4.1 Návrh rozdělení sítě (vlastní)

Demilitarizovaná zóna (DMZ)

Hraniční router i ve stávající architektuře sítě hrál roli hrdla. Jestliže pak tímto bodem prochází veškerý provoz firemní sítě je potřeba pro zvýšení bezpečnosti vnitřní sítě firmy zapnout rozhraní v tomto stávajícím hraničním routeru – firewallu Zyxel Zywall 70, které se nazývá demilitarizovaná zóna (DMZ), jež je součástí tohoto zařízení. Dále se v tomto routeru nastaví oprávnění, které definuje, že do této demilitarizované zóny firemní LAN je povolen přístup vzdálené plochy notebooku vlastníka potažmo jednatele firmy. Pak v tomto routeru bude také povoleno Internetu komunikovat se servery, které jsou zapojeny v této zóně firemní LAN, což zahrnuje webový server, poštovní server a formulářový server. Touto demilitarizovanou zónou se tudíž striktně oddělí Internet od vnitřní sítě firmy a veškerá komunikace ze strany Internetu bude zásadně jen s touto vyhrazenou zónou.

Z toho vyplývá, že se požadavky kladené Internetem nedostanou do samotné vnitřní sítě. Další výhodou zavedení této zóny, kromě lepšího zabezpečení vnitřní sítě firmy, je lepší a přehlednější dohled nad tím, co se v dané interní síti děje a tudíž je možné ji lépe řídit.

Vnitřní síť LAN

Interní router je bránou mezi Internetem, DMZ a vnitřní sítí. Jedná se o zařízení, ve kterém je nutno nastavit oprávnění, jež zakazuje jakémukoliv požadavku z Internetu či demilitarizované zóny vstoupit do interní sítě LAN, pokud tento požadavek nebyl vyžádán přímo touto vnitřní sítí. Naopak je také nutné nastavit oprávnění, že je vnitřní síti povoleno vstupovat jak do demilitarizované zóny, tak na Internet.

Dalším oprávnění vstupu je pak nutno povolit u vzdálené plochy, přes kterou přistupuje k firemní síti vlastník – jednatel firmy a povolit přístup k firemním databázím protokolem HTTPS. U přístupu k firemním databázím se musí dále nastavit oprávněná jen pro pořizování dat, prohlížení těchto dat a vytváření z těchto dat výstupní sestavy.

Rozdělení sítě

V důsledku zavedení demilitarizované zóny se síť rozdělila na dvě podsítě, jak je zřetelné z obrázku 4.1. Jedná se o podsíť demilitarizované zóny a samotnou vnitřní podsíť. Díky tomuto rozdělení sítě na podsítě je komunikace mezi těmito segmenty firemní sítě zredukována na nezbytnou komunikaci, kde její parametry a oprávnění jsou nastavena na vnitřním routeru.

Jelikož se jedná o dvě rozdílné podsítě je potřeba tyto podsítě odrazit i v IP adresách jednotlivých zařízení. IP adresy demilitarizované zóny firemní sítě je možné nastavit staticky přímo na severech. Tyto definované IP adresy DMZ budou nastaveny následovně:

Podsíť	Místnost	Zařízení	IP adresa	Maska
DMZ	Serverovna	Hranový router	192.168.0.1	255.255.255.0
		Formulářový server	192.168.0.2	255.255.255.0
		Poštovní server	192.168.0.3	255.255.255.0
		Webový server	192.168.0.4	255.255.255.0

4.1 IP adresy a maska DMZ (vlastní)

Z tabulky 4.1 lze vysledovat, že IP adresy demilitarizované zóny a tudíž první podsítě firmy jsou v rozsahu 192. 168.0.1 až 192.168.0.255 se stejnou maskou podsítě pro všechny zařízení 255.255.255.0. Je pravidlem nechávat první IP adresu (tady ve tvaru 192.168.1.1) routeru a tady tomu není jinak. Tato IP adresa je přidělena hraničnímu routeru.

Jak je zřejmé z níže uvedené tabulky 4.2 opět je první IP adresa přidělena tentokrát vnitřního routeru ve tvaru 192.168.1.1 s maskou 255.255.255.0 stejnou s demilitarizovanou

zónou firemní sítě. Pak je rozsah IP adres v této druhé vnitřní podsíti firemní LAN stanoven na 192. 168.1.1 až 192.168.1.255.

IP adresy ve vnitřní podsíti se budou lišit, jak je zřejmé z níže uvedené tabulky 4.2.

Podsíť	Místnost	Zařízení	IP adresa	Maska
Vnitřní podsíť LAN	Serverovna	Interní router	192.168.1.1	255.255.255.0
		Databázový server	192.168.1.2	255.255.255.0
		Souborový server	192.168.1.3	255.255.255.0
		Zálohovací server	192.168.1.4	255.255.255.0
	Kancelář 1	Počítač 1	192.168.1.5	255.255.255.0
	Kancelář 2	Počítač 2	192.168.1.6	255.255.255.0
		Počítač 3	192.168.1.7	255.255.255.0
	Kancelář 3	Počítač 4	192.168.1.8	255.255.255.0
	Kancelář 4	Počítač 5	192.168.1.9	255.255.255.0
		Počítač 6	192.168.1.10	255.255.255.0
		Počítač 7	192.168.1.11	255.255.255.0
	Kancelář 5	Počítač 8	192.168.1.12	255.255.255.0
		Počítač 9	192.168.1.13	255.255.255.0
		Počítač 10	192.168.1.14	255.255.255.0
		Počítač 11	192.168.1.15	255.255.255.0
	Kancelář 6	Počítač 12	192.168.1.16	255.255.255.0
	Kancelář 7	Počítač 13	192.168.1.17	255.255.255.0
	Kancelář 8	Počítač 14	192.168.1.18	255.255.255.0
	Kancelář 9	Počítač 15	192.168.1.19	255.255.255.0

4.2 IP adresy a maska vnitřní podsítě LAN (vlastní)

4.3 Šifrovací řešení

V dané firmě mají veškeré počítače i servery souborový systém NTFS, který automaticky zahrnuje i šifrovací systém. Tento šifrovací systém využívá technologii veřejného klíče, jenž chrání data před zneužitím pomocí zašifrování dat. Tato funkce se může, ale také nemusí využívat. Pokud nebude šifrování, které je součástí systému NTFS, nedostačující jednoduše nainstalujeme do počítačového systému jiný šifrovací systém. Například asymetrické šifrování SSL, které firmy využívá pro šifrování dokumentů volané protokolem HTTPS.

Pro zaštítění komunikace mezi DMZ a vnitřní sítí LAN je možné použít síťový autentizační systém Kerberos, jelikož tento mechanismus je přímo podporován Windows Server 2008 R2 Standard a také ho podporuje Linuxový operační systém Debian 4.0

GNU/Linux použitý ve firmě. Ale tento šifrovací systém by výrazně zpomalil celou firemní síť. A vzhledem na velikost firmy to není přímou nezbytností.

Šifrovat by se ale měla zálohovaná data, která jsou ukládána v externích úložištích mimo firmu. Pro tato data by byl vhodný hashovací algoritmus. Například MD5, který je jeden z nejpoužívanějších šifer tohoto druhu.

4.4 Zálohování dat

Zálohování na vysokokapacitní, přepisovatelné páskové záznamové médium je v dnešní době stále nejvýhodnější jak z pohledu kapacitních možností, kde se nabízejí kapacity těchto medií v hodnotách stovek Giga bajtu a jednotkách Tera bajtů, tak její cenové dostupnosti a životnosti pohybující se v řádech desítek let. Tudíž není potřeba měnit v dané firmě zálohovací systém se zálohovací metodou D2D2T.

V důsledku rozšiřování pole působnosti a s narůstající množství dat by si měla firma pořídit další dva pevné disky, které umožňují zapojení do RAID polí.

První disky bude přiřazen databázovému serveru a zapojen do RAID 0, který jen zvyšuje kapacitu spolu i s rychlostí doby přistupování při čtení a zapisování dat, bohužel tento typ RAID pole nezahrnuje i zabezpečení před ztrátou dat, která může nastat při havárii jednoho z disků. Proto jsou prováděny každý den bezpečnostní zálohy na záložní server, kde bude také implementován druhý disk do stávajícího diskového pole RAID 5.

Z důvodu větší bezpečnosti dat je možné přenastavit toto RAID pole typu 5 na RAID 6, který je založena na stejném principu jako RAID5 s tím, že vytváří dvě nezávisle paritní data, díky kterým lze při zhavarování v tomto případě až tří disků ztracená data dopočítat.

Toto přenastavení se provádí v BIOSu daného severu. Při nastavení jednotlivých disků je pak důležité v programu řadiče RAID funkci disku a stanovení hierarchie disků, což je chápáno, že se stanoví, který disk je výchozí, a který cílový.

4.5 Metoda antivirového zabezpečení

Metoda komplexního nasazení antivirového softwaru od jediného poskytovatele ESET na všech úrovních systému má nevýhodu v tom, že je firma zcela závislá na tomto výrobci. Tím je myšleno na jedné virové databázi, kde jsou aktualizace nových virových hrozeb od sebe v dlouhých časových intervalech. Tyto časové intervaly je možné zkrátit pomocí metody

komplexního nasazení antivirového softwaru od různých poskytovatelů. Hlavním distributorem antivirového softwaru by měl zůstat ESET se svým antivirovým balíčkem ESET Secure Business. Ale z důvodů výsledů posledních měření zobrazeny v tabulce 4.3, kdy si ESET na úrovni uživatelských stanic nevedl moc dobře, měl být vybrán nový antivirový program, který bude chránit úroveň koncových stanic. Nejlépe v testu, který se uskutečnil v březnu 2013 (Můj soubor, 2013), dopadl antivirový program AVIRA Antivirus Premium 2013 a druhý solidní antivirový program Kaspersky Anti-Virus 2013.

	Jména antivirových programů	Odhalení škodlivých programu v %	Počet falešných poplachů
1.	G DATA 2013	99.9 %	19
2.	AVIRA	99.6 %	8
3.	F-Secure	99.5 %	11
4.	Bitdefender	99.3 %	9
5.	eScan	99.3 %	21
6.	BullGuard	99.3 %	9
7.	Panda	99.3 %	28
8.	Emsisoft	99.3 %	38
9.	Kaspersky	99.2 %	6
10.	Fortinet	98.6 %	5
11.	Vipre	98.6 %	30
12.	AVG	98.4 %	21
13.	Trend Micro	98.4 %	22
14.	Sophos	98.0 %	6
15.	McAfee	98.0 %	15
16.	Avast	97.8 %	14
17.	ESET	97.5 %	9
18.	AhnLab	92.3 %	19
19.	Microsoft	92.0 %	0
20.	Symantec	91.2 %	23

4.3 Porovnání antivirů 2013 (Můj soubor, 2013)

4.6 Zhodnocení přínosů

První přínosem je detailní **analýza hrozeb a zranitelností** vybrané firmy, tudíž bude firma obeznámena s jejími riziky, které si třeba ani neuvědomovala a tudíž bude dávat větší pozor na své zranitelnosti a v dostatečném předstihu aplikovat opatření vůči vyskytujícím se hrozbám, které zatím neudeřily.

Přínosem **demilitarizované zóny** je lepší zabezpečení firemní, interní počítačové sítě tím, že se tato podsíť oddělí od podsítě DMZ a i samotné externí sítě. K lepšímu zabezpečení

přispívá fakt, že tato podsíť je izolovaná od vnějšího světa, z čehož vyplývá, že požadavky ze strany externí sítě (Internet) nebo i demilitarizované zóny neproniknou do vnitřní sítě firmy, pokud nejsou samozřejmě touto vnitřní firmou přímo vyžádány. Na druhou stranu vnitřní podsíť firmy nemá problém s komunikací s demilitarizovanou zónou nebo Internetem.

S implementováním demilitarizované zóny souvisí i rozdělení firemní sítě na dvě podsítě s odlišnými IP adresami.

Celá tato implementace DMZ, nastavení IP adres a definování oprávnění na routerech počítačové sítě bude potřebovat určitý čas, hlavně z důvodu, že firma IP adresy chce nastavovat staticky. Z hlediska financí je nutné do této demilitarizované zóny pořídit nový router – firewall, který bude hrát roli brány mezi interní podsítí a DMZ s Internetem. Z důvodů dobrých zkušeností firmy by tímto routerem mohl být zase Zyxel Zywall 70, který vlastní i potřebné parametry.

Dalším přínosem tohoto návrhu je zvýšení **bezpečnosti zálohovaných dat** ať už ze strany zašifrování externích záloh pomocí hash algoritmu nebo v podobě diskového pole typu RAID 6, který je sice založen na stejném principu jako RAID 5 a také je o něco málo pomalejší při zápisu, ale je tento RAID spolehlivější a bezpečnější z důvodu pořizování dvojitých paritních informací. Z časového hlediska není aplikování RAID polí tak náročné jako předešlá implementace DZM.

Pomocí šifrování pomocí MD5 zaručí, že data jsou nečitelná pro všechny, co nemají příslušný klíč. A díky tomu že nelze matematicky ani jinak bez klíče dešifrovat, není možné aby tato data bez klíče někdo zneužil.

Antivirová ochrana je stále velice důležitá a aplikování antivirového zabezpečení od více výrobců na různých úrovních struktury umožňuje zvýšit bezpečnost před napadením počítačové sítě viry a jinými infekcemi, které by pak ohrožovaly data. Tato metoda antivirové ochrany od více poskytovatelů je výhodná hlavně ve snížení doby mezi aktualizováním virové databáze, kterou každý poskytovatel aktualizuje v jiných časových intervalech. Tudíž je menší šance, že firemní síť bude napadena neznámým virem či jinou infekcí. Na druhou stranu je tato metoda antivirového zabezpečení poměrně drahá. Proto by firma měla důkladně vybírat tyto poskytovatele antivirového zabezpečení, kde by vždy zhodnotila procento odhalení škodlivých programů v poměru s jejich cenou.

Celý tento návrh by měl poměrně snížit riziko ohrožení prvků firemní počítačové sítě jak z pohledu hardwarového, tak i z pohledu softwaru a dat.

5 Závěr

Každá firma v dnešní době si je vědoma ceny svých chráněných dat a tudíž praktikují jistá opatření, kterými tato data chrání a stejně tak to dělá i firma analyzovaná touto bakalářskou prací. Tato firma operuje v oblasti správy nemovitostí města či jednotlivých majitelů bytů. Pracuje tedy s velmi citlivými daty, jako jsou rodná čísla, čísla účtů, finanční transakce a další.

Prvním cílem této práce tedy bylo analyzovat aktiva a stávající zabezpečení vybrané firmy. Touto analýzou se zabývá celá třetí kapitola. V průběhu zpracovávání této části analýzy byly nalezeny nedostatky v architektuře počítačové sítě. Dále bylo zjištěno, že firma kromě ojedinělých operací nepoužívá žádné bezpečnostní šifrování. Také bylo odhaleno, že veškerou antivirovou ochranu má pod správou jediný poskytovatel, tudíž existuje jen jedna virová databáze.

Druhým a rozsáhlým cílem této práce bylo podrobně analyzovat rizika, hrozby i zranitelná místa této firmy a z těchto analýz vytvořit návrh efektivnějšího zabezpečení prvků dané lokální počítačové sítě. Tyto cíle jsou řešeny ve čtvrté kapitole, kde byl zjištěn fakt, že i přes malou velikost firmy hrozí této firmě velké množství hrozeb a zranitelností. Jednou z přínosů této bakalářské práce je samotné odhalení hrozeb a zranitelností, protože teď si je může firma uvědomit a bránit se proti nim.

Mezi návrh zabezpečení spadá hlavně implementace demilitarizované zóny do architektury firemní sítě a tudíž zajištění vyšší bezpečnosti. Vyšší bezpečnost z pohledu dat zaručuje uplatnění spolehlivějšího typu diskového pole a také zašifrování zálohovaných dat, které jsou odesílány z bezpečnostních důvodů mimo firmu. Nakonec bylo navrženo použití více antivirových systémů, které by zabezpečovali různé úrovně počítačové sítě, z čehož vyplývá, že se zkrátí doba mezi aktualizováním virové databáze, tudíž se snižuje riziko virového napadení počítačové sítě novým virem.

Ovšem postupem času se teprve zjistí, jestli tento návrh řešení nalezených nedostatků skutečně přináší tu míru zabezpečení, jaká byla očekávána nebo jestli není nějaké zabezpečení zbytečné.

Seznam použité literatury

BOUŠKA, Petr. Počítačové sítě - základní topologie. In: *Www.samuraj-cz.com* [online]. 2009 [cit. 2013-03-16]. Dostupné z: http://www.samuraj-cz.com/clanek/pocitacove-site-zakladni-topologie/

ČESKÝ WEBHOSTING S.R.O. *Joomla 2.5.* In: *Návody C4* [online]. © 2007–2013 [cit. 2013-04-20]. Dostupné z: http://navody.c4.cz/joomla-2-5

ČSN ISO/IEC 27000. Informační technologie - Bezpečnostní techniky - Systém řízení bezpečnosti informací - Přehled a Slovník. Praha: Normservis s.r.o., 2010.

ČSN ISO/IEC 27005. Informační technologie - Bezpečnostní techniky - Řízení rizik bezpeřnosti informací. Praha: Normservis s.r.o., 2009.

Debian GNU/Linux 4.0 uvolněn. DEBIAN. *Debian* [online]. 2007 [cit. 2013-04-28]. Dostupné z: http://www.debian.org/News/2007/20070408.cs.html

ESET. *Eset Secure Business* [online]. 2012 [cit. 27-4-2013]. Dostupné z: http://static3.esetstatic.com/fileadmin/Images/CZ/dokumenty/2012/ESB-datasheet-CZ-v03.pdf

HORÁK, Jaroslav. *Hardware: Učebnice pro pokročilé*. 4. vyd. Brno: Computer Press, a.s., 2007. ISBN 978-80-251-1741-5.

KÁLLAY, Fedor a Peter PENIAK. *Počítačové sítě a jejich aplikace*. 2. vyd. Praha: Grada, 2003. ISBN 80-247-0545-1.

LINUXZONE. GAŠPAROVIČ, Petr. *Elektronická pošta v TCP/IP [2] - Referenční model ISO/OSI* [online]. 2004 [cit. 2013-05-06]. Dostupné z: http://www.linuxzone.cz/index.phtml?idc=1132&ids=4

LUDVIG, Miroslav a Bohumír ŠTĚDROŇ. *Teorie bezpečnosti počítačových sítí*. Kralice na Hané: Computer Media, 2008. ISBN 978-80-86686-35-6.

MICROSOFT. *Jak se liší směrovače, rozbočovače, přístupové body a přepínače?* [online]. © 2013 [cit. 2013-04-24]. Dostupné z: http://msdn.microsoft.com/cs-cz/library/ff649429.aspx

MICROSOFT CORPORATION. Kerberos Technical Supplement for Windows [online]. 2005 [cit. 2013-04-24]. Dostupné z: http://msdn.microsoft.com/cs-cz/library/ff649429.aspx

MINISTR, Jan. *Bezpečnost počítačové sítě.* [online]. ©2013 [cit. 2013-04-23]. Dostupné z: http://lms.vsb.cz/mod/resource/view.php?id=9418

MINISTR, Jan. *Informatika: Informační bezpečnost* [online]. 2011 [cit. 20-3-2013]. Dostupné z: http://www.ivsosoom.cz/_doc_download.php?idd=15

MITCHELL, Dave. ZyXEL ZyWALL 70 review. In: *PCpro* [online]. 2005 [cit. 2013-04-20]. Dostupné z: http://www.pcpro.co.uk/reviews/security-appliances/77725/zyxel-zywall-70

Můj soubor. AV COMPARATIVES. *Test nejlepších antivirů – březen 2013* [online]. 2013 [cit. 2013-04-28]. Dostupné z: http://mujsoubor.cz/magazin/test-nejlepsich-antiviru-brezen-2013

PELIKÁN, Jaroslav. *Hardware počítačových sítí* [online]. 2004 [cit. 16-3-2013]. Dostupné z: http://www.fi.muni.cz/usr/pelikan/Vyuka/BHWS/Predn1/Prezent.pdf

PETERKA, Jiří. Elektronická pošta II. In: EArchiv.cz: archiv článků a přednášek Jiřího Peterky [online]. © 2011 [cit. 2013-02-23]. Dostupné z: http://www.earchiv.cz/a94/a409c110.php3

PETŘÍKOVÁ, Jiřina. *Řízení informační bezpečnosti v organizaci*. [online]. 2011 [cit. 2013-04-24]. Dostupné z: http://www.cssi-morava.cz/new/doc/IT2011/petrikova.pdf

Připojení ke vzdálené ploše. MICROSOFT. *Windows* [online]. © 2013 [cit. 2013-05-07]. Dostupné z: http://windows.microsoft.com/cs-cz/windows7/products/features/remote-desktop-connection

SISONSKY, Barrie. *Mistrovství – počítačové sítě.* Brno: Computer Press, a.s., 2010. ISBN 978-80-251-3363-7.

SZOR, Peter. *Počítačové viry: analýza útoku a obrana*. Brno: Zoner Press, 2006. ISBN 80-86815-04-8.

THOMAS, Thomas M. *Zabezpečení počítačových sítí: bez předchozích znalostí*. Brno: CP Books, 2005. ISBN 80-251-0417-6.

VÝŠEK, Ondřej. Porovnání Windows XP / Windows Vista / Windows 7. *Optimalizované IT* [online]. 2009 [cit. 2013-04-28]. Dostupné z: http://www.optimalizovane-it.cz/windows-7/porovnani-windows-xp-/-windows-vista-/-windows-7.html

Zálohování dat. *Xanadu a.s.* [online]. © 2013 [cit. 2013-04-27]. Dostupné z: http://www.xanadu.cz/cs/it-produkty/serverova-reseni/zalohovani-a-archivace/#D2D2T

Seznam zkratek

3DES	Triple Data Ecvryption Standart
ACL	Access Control List
AES	Advanced Ecryption Standart
AS	Authentication Service
ATM	Asynchronous Transfer Mode
BIOS	Basic Input-Output System
BNC	Bayonet Neill-Concelman
BootP	Bootstrap Protocol
CD-R	Compact Disk - Recordable
CD-RW	Compact Disk ReWritable
CMOT	Common Management over TCP/IP
CSV	comma-separated values
D2D2T	Disk-to-Disk-to-Tape
DES	Data Encryption Standart
DHCP	Dynamic Host Configuration Protocol
D-H-M	Diffie-Hellmanův algoritmus
DMZ	Demilitarizovaná zóna
DNS	Domain Name System
DSL	Digital Subscriber Line
EGP	Exterior Gateway Protocol
ELAP	EtherTalk Link Access Protocol
EMI	Elektromagnetická interference
FTP	File Transfer Protocol
HTTP	Hypertext Transport Protocol
HTTPS	Hypertext Transfer Protocol Secure
ICMP	Internet Control Message Protocol
iDES	Internetový Domovní Evidenční Systém
IP	Internet Protocol
IPsec	Internet Protocol Security
ISMS	Information security management system
ISO/IEC	International Organization for Standardization/International Electrotechnical Commission
IT	Informační technologie
KDC	Key distribution center
LAN	Local Area Network
LSA	Local Security Authority
MAN	Metropolitan Area Network
MD5	Message Digest 5
MTA	Massage Transfer Agent
MTS	Message Transfer System

NAT	Network address translation
NFS	Network File System
NNTF	Network News Transfer Protocol
NOS	Network Operating System
NSA	National Security Agency
NTFS	New Technology File System
NTP	Network Time Protocol
OSI	Open Systems Interconnection model
OSPF	Open Shortest Path First
PAN	Personal Area Network
PDF	Portable Document Format
PPP	Point-to-Point Protocol
RAID	Redundant Array of Inexpensive/Independent Disks
RC4	Message Digest 4
RIP	Routing Information Protocol
RPC	Real-time Transport Protocol
RSA	autoři R. Rivest, A. Shamir, L. Adleman
SHA	Secure Hash Algorithm
SLIP	Serial Line Internet Protocol
SMTP	Simple Mail Transfer Protocol
SNTP	Standard Network Time Protocol
SPI	Serial Peripheral Interface Bus
SSL	Secure Sockets Layer
STP	Shielded Twisted-Pair
TELNET	Telecommunication Network
TFTP	Trivial File Transfer Protocol
TGS	Ticket Granting Service
TLAP	TokenTalk Link Access Protocol
UA	User Agent
UDP	User Datagram Protocol
UPS	Uninterruptible power supply
USB	Universal Serial Bus
UTP	Unshielded Twisted-Pair
VHD	Virtual Hard Disk
VPN	Virtual private network
WAN	Wide Area Network
WEP	Wired Equivalent Privacy
WPA	Wi-Fi Protected Access
WWW	World Wide Web
XOR	Bitová nonekvivalence
ZIP	souborový formát

Prohlášení o využití výsledků bakalářské práce

Prohlašuji, že

- jsem byla seznámena s tím, že na mou bakalářskou práci se plně vztahuje zákon č. 121/2000 Sb. – autorský zákon, zejména § 35 – užití díla v rámci občanských a náboženských obřadů, v rámci školních představení a užití díla školního a § 60 – školní dílo;
- beru na vědomí, že Vysoká škola báňská – Technická univerzita Ostrava (dále jen VŠB-TUO) má právo nevýdělečně, ke své vnitřní potřebě, bakalářskou práci užít (§ 35 odst. 3);
- souhlasím s tím, že bakalářská práce bude v elektronické podobě archivována v Ústřední knihovně VŠB-TUO a jeden výtisk bude uložen u vedoucího diplomové (bakalářské) práce. Souhlasím s tím, že bibliografické údaje o bakalářské práci budou zveřejněny v informačním systému VŠB-TUO; bylo sjednáno, že s VŠB-TUO, v případě zájmu z její strany, uzavřu licenční smlouvu s oprávněním užít dílo v rozsahu § 12 odst. 4 autorského zákona;
- bylo sjednáno, že užít své dílo, bakalářskou práci, nebo poskytnout licenci k jejímu využití mohu jen se souhlasem VŠB-TUO, která je oprávněna v takovém případě ode mne požadovat přiměřený příspěvek na úhradu nákladů, které byly VŠB-TUO na vytvoření díla vynaloženy (až do jejich skutečné výše).

V Ostravě dne 7. 5. 2013

Aneta Večeřalová

jméno a příjmení studenta

Seznam příloh

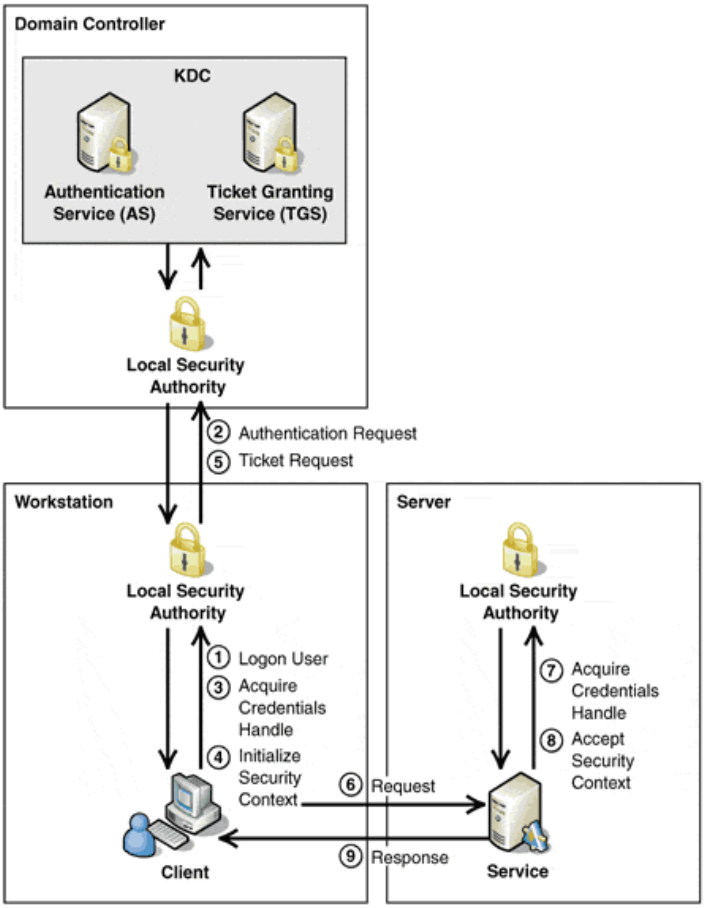
Přílohy - obrázky

Přílohy – tabulky

Přílohy

Přílohy - obrázky

Obrázek 1 Fungování protokolu Kerberos v Microsoft Windows Server 2008



Fungování protokolu Kerberos v Microsoft Windows Server 2008 (Microsoft Corporation, 2005, Dostupné z: http://msdn.microsoft.com/cs-cz/library/ff649429.aspx)

Logon User – uživatel se přihlásí do sítě a jeho přihlašovací informace jsou zaslány serveru místní bezpečnostní autority (LSA, Local Security Authority).

Authentication Request – LSA odevzdá požadavek autentizačníí službě (AS, Authentication Service) spolu s prosbou o autentizaci a ta je uživateli serverem LSA schválena.

Acquire Credentials Handle – LSA zašle náležitá oprávnění uživateli

Initialize Security Context – uživatel začne samotnou relaci.

Ticket Request – uživatel vyžaduje od LSA pro určitou relaci, aplikaci či operaci. Tato žádost postupuje ke službě poskytující lístky (TGS, Ticket Granting Service). Tato služba vytvoří lístek a posílá ho zpátky uživateli.

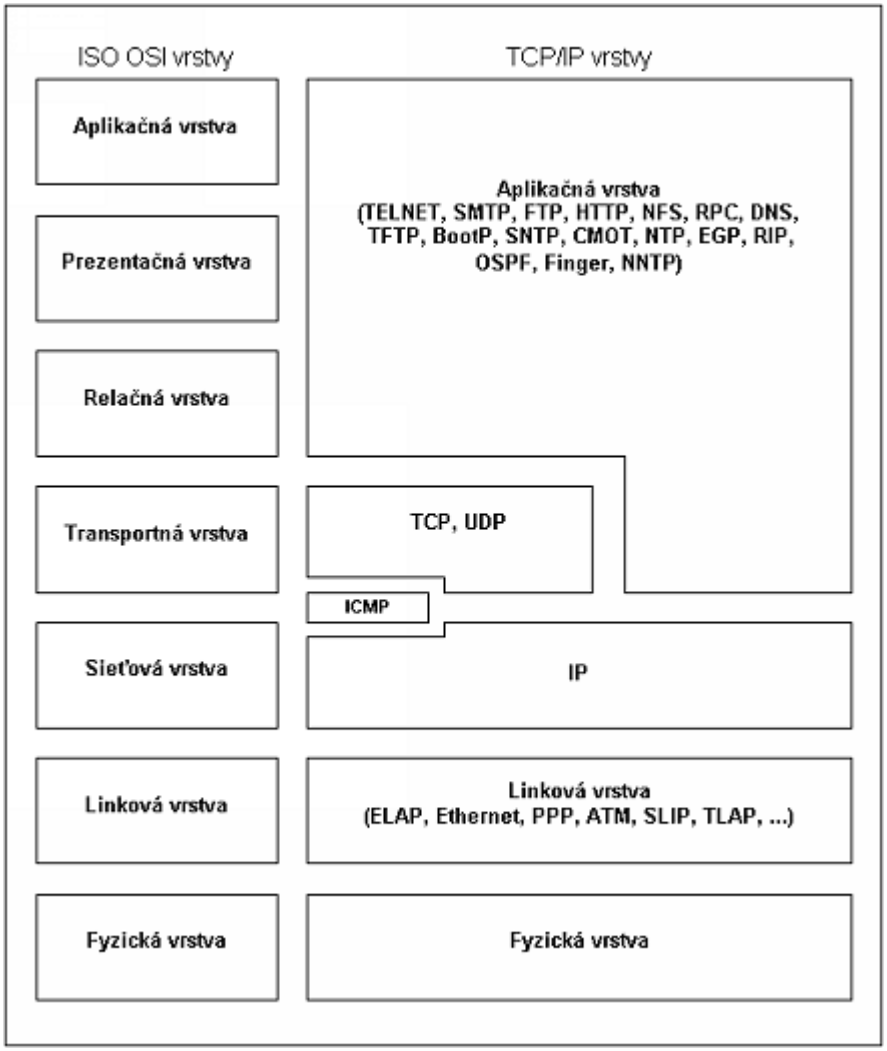
Request – uživatel začíná komunikovat se serverem.

Acquire Credentials Handle – daný server zasílá požadavek LSA pro získání oprávnění uživateli zaslat požadované informace.

Accept Security Context – LSA zašle náležitá oprávnění serveru

Response – server odpoví uživateli na vyžádané informace.

Obrázek 2 Model OSI



(Gašparovič, 2004, Dostupné z: http://www.linuxzone.cz/index.phtml?idc=1132&ids=4)

Obrázek 3 Příklady typických hrozeb 1/2

Typ	Hrozby	Zdroj
Fyzické poškození	Požár	A, D, E
	Poškození vodou	A, D, E
	Znečištění	A, D, E
	Závažná nehoda	A, D, E
	Zničení zařízení nebo médií	A, D, E
	Prach, koroze, zamrznutí	A, D, E
Přírodní události	Klimatický jev	E
	Seizmický jev	E
	Sopečný jev	E
	Meteorologický jev	E
	Povodeň	E
Ztráta základních služeb	Selhání klimatizace nebo dodávky vody	A, D
	Přerušení dodávky elektřiny	A, D, E
	Selhání telekomunikačního zařízení	A, D
Poruchy způsobené zářením	Elektromagnetické záření	A, D, E
	Termální záření	A, D, E
	Elektromagnetické impulzy	A, D, E
Ohrožení informací	Zachycení kompromitujících interferenčních signálů	D
	Vzdálená špionáž	D
	Odposlech	D
	Krádež médií nebo dokumentů	D
	Krádež zařízení	D
	Zprovoznění recyklovaných nebo vyřazených médií	D
	Vyzrazení	A, D
	Data pocházející z nedůvěryhodných zdrojů	A, D
	Falšování pomocí technického vybavení	D
	Falšování pomocí aplikačního programového vybavení	A, D
	Odhalení pozice	D
Technická selhání	Selhání zařízení	A
	Chybné fungování zařízení	A
	Přetížení informačního systému	A, D
	Chybné fungování aplikačního programového vybavení	A
	Chyba údržby	A, D
Neoprávněné činnosti	Neoprávněné použití zařízení	D
	Podvodné kopírování aplikačního programového vybavení	D
	Použití padělaného nebo zkopírovaného aplikačního programového vybavení	A, D
	Poškození dat	D
	Nezákonné zpracování dat	D
Ohrožení funkčnosti	Chyba v používání	A
	Zneužití oprávnění	A, D
	Falšování práv	D
	Odepření činností	D
	Nedostatek personálu	A, D, E

(ISO 27005, s.39, 2009)

A = náhodný

D = úmyslný

E = environmentální

Obrázek 4 Příklady typických hrozeb 2/2

Zdroj hrozby	Motivace	Možné důsledky
Hacker, cracker	Výzva Ego Rebelie Prestiž Peníze	• Hacking • Sociální inženýrství • Narušení a prolomení systému • Neoprávněný přístup do systému
Počítačová kriminalita	Zničení informací Nezákonné prozrazení informací Finanční prospěch Neoprávněné vyzrazení dat	• Počítačový zločin (například kybernetické pronásledování) • Podvodné jednání (například odpovídání, imitace, zachycení) • Získání informace za úplatu • Spoofing • Průnik do systému
Terorismus	Vydírání Zničení Vykořisťování Odplata Politický prospěch Zviditelnění v médiích	• Bombové útoky/Terorismus • Informační válka • Útok na systém (například útok odmítnutí služby, DoS) • Průnik do systému • Porušení systému
Průmyslová špionáž (zpravodajské služby, společnosti, zahraniční vlády, ostatní vládní zájmy)	Konkurenční výhoda Ekonomická špionáž	• Vojenské zvýhodnění • Politické zvýhodnění • Ekonomické zneužití • Krádež informací • Průnik do soukromí • Sociální inženýrství • Průnik do systému • Neoprávněný přístup do systému (přístup ke klasifikovaným aktivum a technologickým informacím
Interní pracovníci (špatně zaškolení, nespokojení, škodolibí, nedbalí, nečestní nebo zaměstnanci s ukončeným pracovním poměrem)	Zvědavost Ego Vyzvědačství Finanční prospěch Odplata Neúmyslné chyby a opomenutí (například Chybné vložení dat, chyba při programování)	• Napadení zaměstnance • Vydírání • Prohlížení chráněných informací • Zneužití počítačů • Podvod a krádež • Získání informace za úplatu • Vložení falešných nebo upravených dat • Narušení komunikace • Škodlivý kód (například virus, logická bomba, trojský kůň) • Prodej osobních údajů • Chyby systému • Průnik do systému • Sabotáž systému • Neoprávněný přístup do systému

(ISO 27005, s.40, 2009)

Obrázek 5 Příklady zranitelností 1/3

Skupiny	Příklady zranitelností	Příklady hrozeb
Hardware	Nedostatečná údržba/chybná instalace záznamových médií	Chyba údržby systému
	Nedodržení pravidelné výměny	Zničení zařízení nebo médií
	Citlivost na vlhkost, prach, zašpinění	Prach, koroze, zamrznutí
	Citlivost na elektromagnetickou radiaci	Elektromagnetické záření
	Nedostatek v účinném nastavení změnového řízení	Chyba použití
	Citlivost na změny napětí	Přerušení dodávky elektřiny
	Citlivost na změny teploty	Meteorologický jev
	Nechráněné uskladnění	Krádež médií nebo dokumentů
	Nedostatečné postupy likvidace	Krádež médií nebo dokumentů
	Nekontrolované kopírování	Krádež médií nebo dokumentů
Software	Žádné nebo nedostatečné testování programů	Zneužití oprávnění
	Známé chyby v programech	Zneužití oprávnění
	Neodhlášení se při opouštění pracovní stanice	Zneužití oprávnění
	Vyřazení nebo opětovné použití záznamových médií bez důkladného vymazání	Zneužití oprávnění
	Neprovádění logování událostí	Zneužití oprávnění
	Chybné přiřazení přístupových práv	Zneužití oprávnění
	Široce rozšířené programy	Poškození dat
	Použití aplikačních programů na špatná data z hlediska času	Poškození dat
	Složité uživatelské rozhraní	Chyba použití
	Nedostatečná dokumentace	Chyba použití
	Špatné nastavení parametrů	Chyba použití
	Nesprávný datum	Chyba použití
	Nedostatečná identifikace a autentizace, například autentizace uživatele	Falšování práv
	Nechráněné tabulky s hesly	Falšování práv
	Špatná správa hesel	Falšování práv
	Spuštění nepotřebných služeb	Nezákonné zpracování dat
	Neodladěný nebo nový program	Chybné fungování aplikačního programového vybavení
	Nejasné nebo neúplné zadání pro vývojáře	Chybné fungování aplikačního programového vybavení
	Nedostatečné řízení změn	Chybné fungování aplikačního programového vybavení
	Nekontrolované stahování a užívání programů	Falšování pomocí aplikačního programového vybavení
	Nedostatečné zálohování	Falšování pomocí aplikačního programového vybavení
	Nedostatečná fyzická ochrana budov, dveří a oken	Krádež médií nebo dokumentů
	Chyba v produkci reportů pro management	Neoprávněné použití zařízení

(pokračování)

(ISO 27005, s.41, 2009)

Obrázek 6 Příklady zranitelností 2/3

(pokračování)

Skupiny	Příklady zranitelností	Příklady hrozeb
Sítě	Nedostatečné ověřování posílání a přijímání zpráv	Odepření činností
	Nechráněné komunikační linky	Odposlech
	Nechráněné citlivý provoz přenosu	Odposlech
	Nekvalitní kabelové spojení	Selhání telekomunikačního zařízení
	Bod totálního selhání	Selhání telekomunikačního zařízení
	Nedostatečná identifikace a autentizace, například Autentizace uživatele	Falšování práv
	Nedostatečně bezpečná síťová architektura	Vzdálená špionáž
	Přenos odkrytých hesel	Vzdálená špionáž
	Nedostatečné řízení sítí (odolnost směrování)	Přetížení informačního systému
	Nechráněné připojení do veřejné sítě	Neoprávněné použití zařízení
Zaměstnanci	Nepřiměřená nebo nedbalá kontrola fyzického přístupu do budov, místností a kanceláří	Nedostatek personálu
	Nedostatečné postupy pro nábor pracovníků	Zničení zařízení nebo médií
	Nedostatečné bezpečnostní školení	Chyba použití
	Nesprávné použití aplikačního programového a technického vybavení	Chyba použití
	Nedostatek povědomí o bezpečnosti	Chyba použití
	Nedostatek kontrolních mechanizmů	Nezákonné zpracování dat
	Nedostatečná kontrola práce externích zaměstnanců nebo zaměstnanců zabezpečujících úklid	Krádež médií nebo dokumentů
	Nedostatek politik pro použití telekomunikačních prostředků a posílání zpráv	Neoprávněné použití zařízení
Lokality	Nepřiměřená nebo nedbalá kontrola fyzického přístupu do budov, místností a kanceláří	Zničení zařízení nebo médií
	Poloha v zátopové oblasti	Povodeň
	Nestabilní elektrická síť	Přerušení dodávky elektřiny
	Nedostatečná fyzická ochrana budov, dveří a oken	Krádež zařízení
Organizace	Nedostatečný formální postup při registraci a zrušení registrace uživatele	Zneužití oprávnění
	Nedostatečný formální postup při revizi uživatelských práv	Zneužití oprávnění
	Nedostatečné nebo neúplné zajištění (bezpečnosti) ve smlouvách se zákazníky a/nebo třetími stranami	Zneužití oprávnění
	Nedostatky v postupech pro monitorování prostředků pro zpracování informací	Zneužití oprávnění
	Nedostatečné provádění pravidelných auditů (dohledu)	Zneužití oprávnění
	Nedostatky v postupech pro identifikaci a hodnocení rizik	Zneužití oprávnění
	Nedostatečné chybové záznamy v logu evidujícím činnosti správců a administrátorů	Zneužití oprávnění
	Nedostatečná odezva pracovníků údržby systému	Chyba údržby systému
	Nedostatečná nebo neúplná smlouva o úrovni služeb	Chyba údržby systému
	Nedostatky v postupech pro řízení změn	Chyba údržby systému
	Nedostatky v postupech pro řízení dokumentace ISMS	Poškození dat
	Nedostatky ve formálních postupech pro revizi záznamů ISMS	Poškození dat
	Nedostatky ve formálním procesu pro autorizaci veřejně přístupných informací	Data pocházející z nedůvěryhodných zdrojů

(pokračování)

(ISO 27005, s.42, 2009)

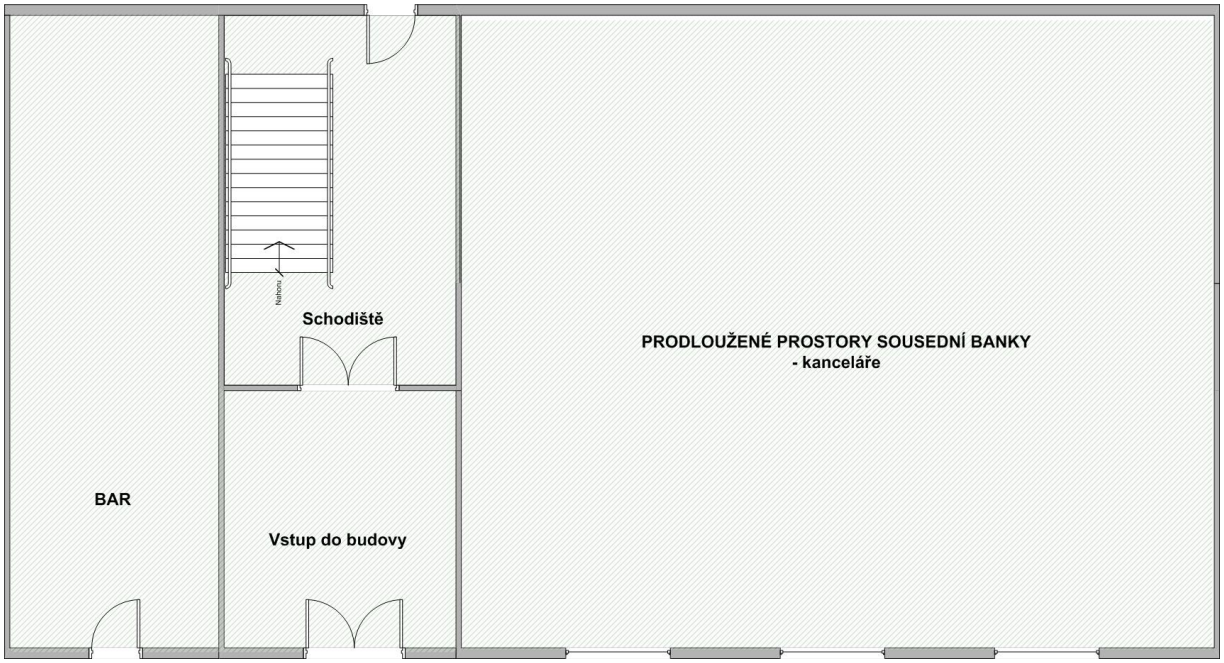
Obrázek 7 Příklady zranitelností 3/3

(dokončení)

Skupiny	Příklady zranitelností	Příklady hrozeb
	Nedostatky ve vhodném přidělení odpovědností za bezpečnost informací	Odepření činností
	Nedostatky v plánech kontinuity	Selhání zařízení
	Nedostatky v politice pro používání emailu	Chyba použití
	Nedostatečné postupy pro instalaci softwaru do operačních systémů	Chyba použití
	Nedostatečné záznamy v logu evidujícím činnosti správců a administrátorů	Chyba použití
	Nedostatky v postupech pro zacházení s klasifikovanými informacemi	Chyba použití
	Nedostatečně definované povinnosti informační bezpečnosti v popisu pracovních pozic	Chyba použití
	Nedostatečné nebo neúplné zajištění (bezpečnosti) ve smlouvách se zaměstnanci	Nezákonné zpracování dat
	Nedostatečně definované disciplinární řízení v případě vzniku incidentu týkajícího se bezpečnosti informací	Krádež zařízení
	Nedostatky ve formální politice pro používání mobilních zařízení	Krádež zařízení
	Nedostatečné kontroly zařízení mimo lokalitu	Krádež zařízení
	Nedostatečné dodržování pravidel prázdného stolu a prázdné obrazovky monitoru	Krádež médií nebo dokumentů
	Nedostatečný schvalovací proces prostředků pro zpracování informací	Krádež médií nebo dokumentů
	Nedostatečně definované monitorovací mechanizmy při narušení bezpečnosti	Krádež médií nebo dokumentů
	Nedostatek v přezkoumáních managementem	Neoprávněné použití zařízení
	Nedostatečné postupy hlášení bezpečnostních slabin	Neoprávněné použití zařízení
	Nedostatečné postupy pro zajištění souladu se zákony na ochranu duševního vlastnictví	Použití padělaného nebo zkopírovaného aplikačního programového vybavení

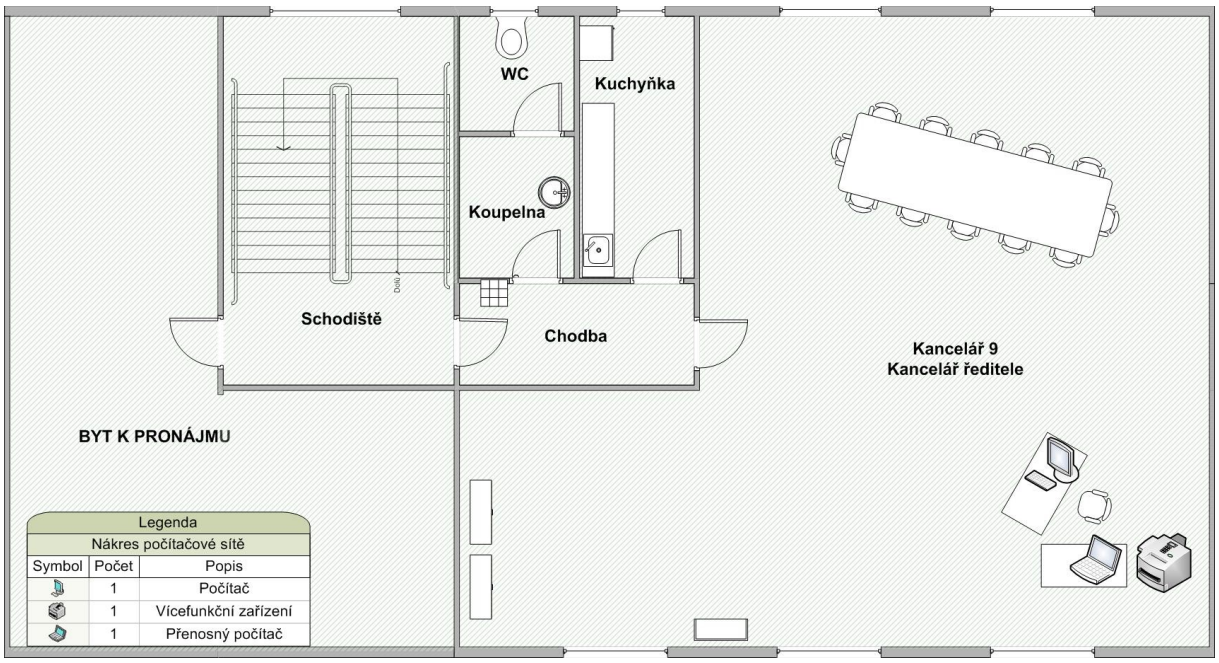
(ISO 27005, s.43, 2009)

Obrázek 8 Přízemí firmy



(vlastní)

Obrázek 9 Třetí patro firmy



(vlastní)

Přílohy – tabulky

Tabulka 1 Výhody a nevýhody koaxiálního kabelu

Výhody	Nevýhody
- poměrně lehká instalace - dobrá cena - slouží i k přenosu zvuku a obrazu - vysoká odolnost vůči EMI	- sklon k poruchovosti - nelze uplatnit v sítích Token-Ring

(vlastní)

Elektromagnetická interference (EMI) – podle Sosinského (2010) se jedná o nahodilou energii z vnějšího zdroje, která způsobuje rušení signálu a snížení kvality komunikace probíhající v elektrických vodičích.

Tabulka 2 Výhody a nevýhody kroucené dvojlinky

Výhody	Nevýhody
- nízká cena - lehká instalace a snadné zapojení - možnost užití i jako jiné propojení (např.: telefon) - STP je velice dobře odolná vůči EMI	- STP je masivní a těžce se s ním pracuje - UTP je vnímavější na šum než koaxiální kabel - UTP signály nemohou být bez obnovy přenášeny na větší vzdálenosti

(vlastní)

Tabulka 3 Typy RAID

Typ	Princip	Výhody	Nevýhody
RAID 0, striping	Data se rozdělují mezi několik disků.	Zvýšení kapacity, snížení přístupové doby při čtecích i zapisovacích operacích.	Nezvyšuje bezpečnost, pokud jeden disk nezhavaruje, ztratíme všechna data.
RAID 1, mirroring	Data se současně zapisují na více disků (většinou dva). Jeden disk je úplnou kopii druhého.	Data jsou 100% redundantní. Vysoká bezpečnost, při poruše primárního disku přebírá jeho funkci sekundární disk. Dochází ke zvýšení čtecích operací díky	Kapacita jednoho disku je zrcadlena na disk další. K uložení dat je tak potřebná dvojnásobná kapacita (2 disky

		současnému čtení ze dvou disků.	
RAID 5, striping s redundancí	Data jsou rozdělována mezi více disků. ‚Nadbytečná' paritní data jsou rozprostřena na všechny disky. Zhavarovaný disk je možné vyměnit. Jeho data jsou pak rekonstruována pomocí paritních redundantních údajů.	Zvýšení výkonu při čtecích operacích. Redundantní data zaberou jen část kapacity disků (není třeba zdvojnásobovat kapacitu disků). Havarovaný disk je možné vyměnit a pole dopočítá a zrekonstruuje chybějící data.	Potřeba minimálně tří disků.
RAID 10 streping s mirroringem (RAID 0 + RAID 1)	Data jsou rozdělována mezi několik disků (RAID 0). Dosáhne se tak vysoké rychlosti. Každý z disků RAID 0 je ještě zrcadlen.	Vysoká rychlost kombinovaná s bezpečností.	Na stripping potřebujeme 2 disky a na zrcadlení další 2 – potřeba minimálně 4 disků.

(Horák, s.205, 2007)

Tabulka 4 Srovnání operačních systémů na stanicích

Kategorie	Vlastnost	Windows XP SP3	Windows Vista SP1	Windows 7
Správa a organizace souborů	Desktop search	Ke stažení	Ano	Vylepšené
	Knihovny	Ne	Ne	Nové
	Federované vyhledávání	Ne	Ne	Nové
	Enterprise Search Scopes (Windows 7 Ultimate/Enterprise + Windows Server 2008 R2)	Ne	Ne	Nové
Vzdálený přístup	DirectAccess	Ne	Ne	Nové
	VPN Reconnect	Ne	Ne	Nové
	BrancCache	Ne	Ne	Nové
	Mobilní širokopásmový přístup	Ne	Ne	Nové
	RemoteApp & připojení desktopu	Ne	Ne	Nové
Bezpečnost	BitLocker	Ne	Ano	Vylepšené
	BitLocker ToGo	Ne	Ne	Nové
	AppLocker	Ne	Ne	Nové
	Více profilů FireWall	Ne	Ne	Nové

	Detailní audit	Ne	Ano	Vylepšené
	User Account Control	Ne	Ano	Vylepšené
	Domain Name System Security Extensions	Ne	Ne	Nové
	Podpora Smart karet	Ano	Ano	Vylepšené
	Podpora Biometriky	Ano, 3.strna	Ano, 3.strana	Nové
Správa	Windows PowerShell v2	Ke stažení	Ke stažení	Již obsaženo
	Skriptování nastavení skupinových politik	Ne	Ne	Vylepšené
	Group Policy preferences	Ke stažení	Ke stažení	Nové
	Windows Recovery Environment	Ne	Ano	Vylepšené
	Platforma pro řešení problémů	Ne	Ne	Nové
	Jednotné trasování	Ano	Ano	Vylepšené
	Záznam problému	Ne	Ne	Nové
	Vzdálený přístup k informacím o spolehlivosti	Ne	Ne	Nové
Nasazení	Deployment image servicing & správa obrazů	Ne	Ano	Vylepšené
	Dynamic Driver Provisioning	Ne	Ne	Nové
	Volume Activation	Ne	Ano	Vylepšené
	Multicast multiple stream transfer	Ne	Ne	Nové
	User State Migration Tool	Ano	Ano	Vylepšené
	Správa a nasazení pomocí VHD	Ne	Ne	Nové
	Možnosti vzdáleného přístupu (Multimedia, obousměrný zvuk, více monitorů)	Ne	Ne	Nové
	VHD boot	Ne	Ne	Nové

(VÝŠEK, 2009, Dostupné z: http://www.optimalizovane-it.cz/windows-7/porovnani-windows-xp-/-windows-vista-/-windows-7.html)